Administrar VMware vSAN

Actualización 3

VMware vSphere 8.0
VMware vSAN 8.0



Puede encontrar la documentación técnica más actualizada en el sitio web de VMware by Broadcom en:

https://docs.vmware.com/es/

VMware by Broadcom
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contenido

Acerca de Administrar VMware vSAN

En *Administrar VMware vSAN*, se describe cómo configurar y administrar un clúster de vSAN en un entorno de VMware vSphere®.

En *Administrar VMware vSAN* también se explica cómo administrar los recursos de almacenamiento físico local que funcionan como dispositivos de capacidad de almacenamiento en un clúster de vSAN. De igual manera, se explica cómo definir directivas de almacenamiento para máquinas virtuales implementadas en almacenes de datos de vSAN.

En VMware, valoramos la inclusión. Para fomentar este principio de forma interna y en nuestra comunidad de clientes y socios, creamos contenido con un lenguaje inclusivo.

Audiencia prevista

Esta información está destinada a administradores de virtualización experimentados que están familiarizados con la tecnología de virtualización, las operaciones cotidianas de los centros de datos y los conceptos de vSAN.

Para obtener más información sobre vSAN y la creación de un clúster de vSAN, consulte la guía *Planificar e implementar vSAN*.

Para obtener más información sobre cómo supervisar un clúster de vSAN y solucionar problemas, consulte la guía *Supervisar vSAN y solucionar sus problemas*.

Información actualizada

1

Este documento se actualiza con cada versión del producto o cuando sea necesario.

Esta tabla brinda información sobre el historial de actualizaciones del documento *Administrar VMware vSAN*.

Revisión	Descripción
25 JUL 2024	■ Se actualizó la información de licencias sobre vSAN Max en Compartir almacenes de datos remotos de vSAN . ■ Se agregó información sobre la restauración de las máquinas virtuales eliminadas en Restaurar una máquina virtual a partir de una instantánea de vSAN. ■ Actualizaciones menores adicionales.
25 de junio de 2024	Versión inicial.

Qué es vSAN

2

VMware vSAN es una capa distribuida de software que se ejecuta de manera nativa como parte del hipervisor de ESXi.

vSAN agrega dispositivos de capacidad locales o con conexión directa de un clúster de host y crea un grupo de almacenamiento individual compartido entre todos los hosts del clúster de vSAN. vSAN admite las características de VMware que requieren almacenamiento compartido (como HA, vMotion y DRS) y, al mismo tiempo, elimina la necesidad de usar almacenamiento compartido externo y simplifica las actividades de aprovisionamiento de máquinas virtuales y configuración de almacenamiento.

Lea los siguientes temas a continuación:

Conceptos de vSAN

VMware vSAN emplea un enfoque definido por software que crea almacenamiento compartido para máquinas virtuales.

Virtualiza los recursos locales de almacenamiento físico de los hosts ESXi y los transforma en grupos de almacenamiento que pueden dividirse y asignarse a máquinas virtuales y aplicaciones en función de sus requisitos de calidad de servicio. vSAN se implementa directamente en el hipervisor de ESXi.

Puede configurar vSAN para que funcione como un clúster híbrido o basado íntegramente en tecnología flash. En clústeres híbridos, se utilizan dispositivos flash para la capa de almacenamiento en caché y discos magnéticos para la capa de capacidad de almacenamiento. En los clústeres basados íntegramente en tecnología flash, los dispositivos flash se utilizan para memoria caché y de capacidad.

Puede activar vSAN en los clústeres de hosts existentes o cuando cree un nuevo clúster. vSAN agrega todos los dispositivos de capacidad a un solo almacén de datos compartido por todos los hosts del clúster de vSAN. Puede expandir el almacén de datos agregando dispositivos de capacidad o hosts con dispositivos de capacidad al clúster. vSAN funciona mejor cuando todos los hosts ESXi del clúster comparten configuraciones similares o idénticas entre

todos los miembros del clúster, lo que incluye configuraciones similares o idénticas para el almacenamiento. Esta configuración coherente equilibra los componentes de almacenamiento de máquinas virtuales en todos los dispositivos y hosts del clúster. Los hosts sin dispositivos locales también pueden participar y ejecutar sus máquinas virtuales en el almacén de datos de vSAN.

En vSAN Original Storage Architecture (OSA), cada host que aporta dispositivos de almacenamiento al almacén de datos de vSAN debe proporcionar al menos un dispositivo para memoria caché flash y al menos un dispositivo para capacidad. Los dispositivos del host que aporta los dispositivos forman un grupo de discos o más. Cada grupo de discos contiene un dispositivo flash de almacenamiento en caché y un dispositivo de capacidad, o varios, para almacenamiento persistente. Cada host puede configurarse para emplear varios grupos de discos.

En vSAN Express Storage Architecture (ESA), todos los dispositivos de almacenamiento reclamados por vSAN contribuyen a la capacidad y el rendimiento. Los dispositivos de almacenamiento de cada host reclamados por vSAN forman un grupo de almacenamiento. El grupo de almacenamiento representa la cantidad de caché y capacidad proporcionadas por el host al almacén de datos de vSAN.

Para obtener información sobre prácticas recomendadas, consideraciones de capacidad y recomendaciones generales sobre el diseño y el dimensionamiento de un clúster de vSAN, consulte la *guía de diseño y dimensionamiento de VMware vSAN*.

Características de vSAN

Las siguientes características se aplican a vSAN, sus clústeres y almacenes de datos.

vSAN incluye numerosas funciones para agregar resistencia y eficiencia a su entorno de almacenamiento y computación de datos.

Tabla 2-1. Características de vSAN

Funciones compatibles	Descripción
Compatibilidad con almacenamiento compartido	vSAN es compatible con funciones de VMware que requieren almacenamiento compartido, como HA, vMotion y DRS. Por ejemplo, si un host está sobrecargado, DRS puede migrar máquinas virtuales a otros hosts del clúster.
Formato en disco	El formato de archivo virtual en disco de vSAN ofrece una administración de instantáneas y clones muy escalable por cada clúster de vSAN. Para obtener información sobre la cantidad de instantáneas y clones de máquinas virtuales que se admite por cada clúster de vSAN, consulte *Valores máximos de configuración* de vSphere https://configmax.esp.vmware.com/home.
Configuraciones híbridas y basadas íntegramente en tecnología flash	vSAN puede configurarse para un clúster híbrido o basado íntegramente en tecnología flash.
Dominios de errores	vSAN admite la configuración de dominios de errores para proteger a los hosts contra errores de los bastidores o los chasis cuando el clúster de vSAN abarca varios bastidores o chasis de servidores blade en un centro de datos.

Tabla 2-1. Características de vSAN (continuación)

Funciones compatibles	Descripción
Servicio de archivos	El servicio de archivos de vSAN permite crear recursos compartidos de archivos en el almacén de datos de vSAN al que pueden acceder las máquinas virtuales o las estaciones de trabajo cliente.
Servicio del destino iSCSI.	El servicio del destino iSCSI de vSAN permite que los hosts y las cargas de trabajo físicas que se encuentren fuera del clúster de vSAN accedan al almacén de datos de vSAN.
Clúster ampliado de vSAN y clúster de vSAN de dos nodos	vSAN admite clústeres ampliados que abarcan dos ubicaciones geográficas.
Compatibilidad con clústeres de conmutación por error de Windows Server (Windows Server Failover Clusters, WSFC)	vSAN 6.7 Update 3 y las versiones posteriores admiten las reservas persistentes de SCSI-3 (SCSI-3 Persistent Reservations, SCSI-3 PR) en el nivel de disco virtual que el clúster de conmutación por error de Windows Server (Windows Server Failover Cluster, WSFC) requiere para arbitrar un acceso a un disco compartido entre nodos. La compatibilidad con instancias de SCSI-3 PR permite la configuración de WSFC con un recurso de disco compartido entre las máquinas virtuales de forma nativa en los almacenes de datos de vSAN. Actualmente se admiten las siguientes configuraciones: ■ Hasta 6 nodos de aplicación por clúster. ■ Hasta 64 discos virtuales compartidos por nodo. **Nota** Microsoft SQL Server 2012, o una versión posterior que se ejecute en Microsoft Windows Server 2012 o posterior, calificó para vSAN.
vSAN Health Service	vSAN Health Service incluye pruebas de comprobación de estado configuradas previamente para supervisar, solucionar problemas, diagnosticar causas de problemas de componentes del clúster e identificar riesgos posibles.
Servicio de rendimiento de vSAN	En el servicio de rendimiento de vSAN, se incluyen tablas estadísticas utilizadas para supervisar las E/S por segundo, el rendimiento, la latencia y la congestión. Puede supervisar el rendimiento de un clúster de vSAN, un host, un grupo de discos, un disco y máquinas virtuales.
Integración con las funciones de almacenamiento de vSphere	vSAN se integra con las funciones de administración de datos de vSphere utilizadas tradicionalmente con el almacenamiento VMFS y NFS. Estas funciones incluyen instantáneas, clones vinculados y vSphere Replication.
Directivas de almacenamiento de máquinas virtuales	vSAN funciona con las directivas de almacenamiento de máquina virtual para admitir un enfoque centrado en máquinas virtuales en la administración de almacenamiento. Si no se asigna una directiva de almacenamiento a la máquina virtual durante la implementación, se asigna automáticamente la directiva de almacenamiento predeterminada de vSAN a la máquina virtual.

Tabla 2-1. Características de vSAN (continuación)

Funciones compatibles	Descripción
Aprovisionamiento rápido	vSAN permite el aprovisionamiento rápido de almacenamiento en vCenter Server® durante las operaciones de creación e implementación de máquinas virtuales.
Desduplicación y compresión	vSAN realiza la desduplicación y la compresión a nivel de bloque para ahorrar espacio de almacenamiento. Cuando se habilitan la desduplicación y la compresión en un clúster basado en flash de vSAN, se reducen los datos redundantes dentro de cada grupo de discos. La desduplicación y la compresión son configuraciones para todo el clúster, pero las funciones se aplican a cada grupo de discos de forma individual. Se aplicará vSAN de solo compresión en cada disco.
Cifrado de datos en reposo	vSAN proporciona el cifrado de datos en reposo. Los datos se cifran después de que se llevan a cabo todas las otras operaciones de procesamiento, como la desduplicación. El cifrado de datos en reposo protege los datos de los dispositivos de almacenamiento, en caso de que un dispositivo se quite del clúster.
Cifrado de datos en tránsito	vSAN puede cifrar los datos en tránsito entre los hosts del clúster. Cuando se habilita el cifrado de datos en tránsito, vSAN cifra todos los datos y el tráfico de metadatos entre los hosts.
Compatibilidad con SDK	VMware vSAN SDK es una extensión de VMware vSphere Management SDK. Incluye documentación, bibliotecas y ejemplos de código que ayudan a los desarrolladores a automatizar la instalación, la configuración, la supervisión y la solución de problemas de vSAN.

Términos y definiciones de vSAN

vSAN introduce términos y definiciones específicos que resulta importante comprender.

Antes de comenzar con vSAN, revise los términos y definiciones clave de vSAN.

Grupo de discos (vSAN Original Storage Architecture)

Un grupo de discos es una unidad de rendimiento y capacidad de almacenamiento físico en un host y un grupo de dispositivos físicos que proporcionan rendimiento y capacidad al clúster de vSAN. En cada host ESXi que aporta sus dispositivos locales a un clúster de vSAN, los dispositivos se organizan en grupos de discos.

Cada grupo de discos debe tener un dispositivo flash de almacenamiento en caché y un dispositivo de capacidad, o varios. Los dispositivos utilizados para el almacenamiento en caché no pueden compartirse entre los grupos de discos ni tampoco pueden utilizarse para otras finalidades. Cada dispositivo de almacenamiento en caché debe estar dedicado a un solo grupos de discos. En clústeres híbridos, se utilizan dispositivos flash para la capa de almacenamiento en

caché y discos magnéticos para la capa de capacidad de almacenamiento. En un clúster basado íntegramente en tecnología flash, los dispositivos flash se utilizan para la memoria caché y la capacidad. Para obtener información sobre la creación y la administración de grupos de discos, consulte *Administrar VMware vSAN*.

Grupo de almacenamiento (vSAN Express Storage Architecture)

Un grupo de almacenamiento es una representación de todos los dispositivos de almacenamiento en un host reclamado por vSAN. Cada host contiene un grupo de almacenamiento. Cada dispositivo del grupo de almacenamiento aporta capacidad y rendimiento. La cantidad de dispositivos de almacenamiento permitidos está determinada por la configuración del host.

Capacidad utilizada

La capacidad utilizada es la cantidad de capacidad física utilizada por una máquina virtual o más en cualquier momento dado. Existen muchos factores que determinan la capacidad utilizada, incluidos el tamaño utilizado de sus archivos `.vmdk`, las réplicas de protección, etc. Al calcular el tamaño de la memoria caché, no tenga en cuenta la capacidad utilizada para las réplicas de protección.

Almacenamiento basado en objetos

vSAN almacena y administra datos en contenedores flexibles de datos denominados objetos. Un objeto es un volumen cuyos datos y metadatos se distribuyen en el clúster. Por ejemplo, cada archivo `.vmdk` constituye un objeto, al igual que cada instantánea. Al aprovisionar una máquina virtual en un almacén de datos de vSAN, vSAN crea un conjunto de objetos compuesto por varios componentes para cada disco virtual. También crea el espacio de nombres del directorio principal de la máquina virtual, el cual es un objeto contenedor que almacena todos los archivos de metadatos de la máquina virtual. Según la directiva de almacenamiento de máquina virtual que se asignó, vSAN aprovisiona y administra cada objeto de manera individual, proceso que también puede incluir la creación de una configuración de RAID para cada objeto.

Nota Si se habilita vSAN Express Storage Architecture, cada instantánea no se considerará un objeto nuevo. Un archivo `.vmdk` base y sus instantáneas estarán contenidos en un objeto de vSAN. Además, en vSAN ESA, el resumen está respaldado por objetos de vSAN.

Cuando vSAN crea un objeto para un disco virtual y determina cómo distribuir el objeto en el clúster, considera los siguientes factores:

- vSAN comprueba que se apliquen los requisitos de discos virtuales de acuerdo con la configuración especificada para la directiva de almacenamiento de máquinas virtuales.

- vSAN comprueba que se utilicen los recursos de clúster correctos durante el aprovisionamiento. Por ejemplo, en función de la directiva de protección, vSAN determina cuántas réplicas se deben crear. La directiva de rendimiento determina la cantidad de Flash Read Cache para cada réplica y, asimismo, la cantidad de fracciones que se deben crear para cada réplica y dónde se deben ubicar dentro del clúster.
- vSAN supervisa e informa constantemente del estado de conformidad de la directiva para el disco virtual. Si encuentra cualquier estado que incumple la directiva, debe realizar un procedimiento de solución de problemas y resolver el problema subyacente.

  Nota Cuando sea necesario, puede editar la configuración de la directiva de almacenamiento de la máquina virtual. La modificación de la configuración de la directiva de almacenamiento no afecta el acceso de la máquina virtual. vSAN regula de manera activa los recursos de red y almacenamiento que se utilizan para la reconfiguración, a fin de reducir el impacto de la reconfiguración de objetos en las cargas de trabajo normales. Cuando se modifica la configuración de la directiva de almacenamiento de máquina virtual, es posible que vSAN inicie un proceso de recreación de objetos y la resincronización posterior. Consulte *Supervisar vSAN y solucionar sus problemas*.

- vSAN comprueba que los componentes de protección necesarios, como los reflejos y los testigos, se coloquen en dominios de errores o en hosts separados. Por ejemplo, para recompilar componentes durante un error, vSAN busca hosts ESXi que cumplan con las reglas de colocación en las que los componentes de protección de objetos de máquinas virtuales deben colocarse en dos hosts diferentes o en dominios de error.

Almacén de datos de vSAN

Después de habilitar vSAN en un clúster, se crea un solo almacén de datos de vSAN. Se muestra como otro tipo de almacén de datos en la lista de los almacenes de datos que pueden estar disponibles, incluidos los volúmenes virtuales, VMFS y NFS. Un solo almacén de datos de vSAN puede proporcionar distintos niveles de servicio para cada máquina o disco virtuales. En vCenter Server®, se muestran las características de almacenamiento del almacén de datos de vSAN como un conjunto de funcionalidades. Al definir una directiva de almacenamiento para máquinas virtuales, puede hacer referencia a estas funcionalidades. Cuando se implementan máquinas virtuales posteriormente, vSAN utiliza esta directiva para colocar las máquinas virtuales en el modo óptimo en función de los requisitos de cada máquina virtual. Para obtener información general sobre el uso de las directivas de almacenamiento, consulte el documento *Almacenamiento de vSphere* .

Un almacén de datos de vSAN posee características específicas que se deben considerar.

- vSAN proporciona un solo almacén de datos de vSAN, al que pueden acceder todos los hosts del clúster, independientemente de si aportan almacenamiento o no al clúster. Cada host puede montar cualquier otro tipo de almacenes de datos, incluidos los volúmenes virtuales, VMFS y NFS.
- Puede usar Storage vMotion para transferir máquinas virtuales entre los almacenes de datos de vSAN, de NFS y de VMFS.

- Solo los discos magnéticos y los dispositivos flash utilizados para capacidad pueden aportar capacidad al almacén de datos. Los dispositivos utilizados para la memoria caché flash no cuentan como parte del almacén de datos.

Objetos y componentes

Cada objeto consta de un conjunto de componentes, determinado por las funcionalidades utilizadas en la directiva de almacenamiento de máquina virtual. Por ejemplo, si **Errores que se toleran** se establece en 1, vSAN garantiza que los componentes de protección (como las réplicas y los testigos) se coloquen en hosts separados del clúster de vSAN, en el que cada réplica es un componente de un objeto. Además, en la misma directiva, si el valor configurado para el **número de fracciones de disco por objeto** es de dos o más, vSAN también fracciona el objeto en varios dispositivos de capacidad y cada fracción se considera un componente del objeto especificado. Cuando es necesario, vSAN también puede dividir los objetos grandes en varios componentes.

Un almacén de datos de vSAN contiene los siguientes tipos de objeto:

Espacio de nombres del directorio principal de la máquina virtual

El directorio principal de máquina virtual en el que se almacenan todos los archivos de configuración de máquina virtual, como `.vmx`, los archivos de registro, los archivos `.vmdk` y los archivos de descripción delta de instantáneas.

VMDK

Un disco de máquina virtual o un archivo `.vmdk` que almacena el contenido de la unidad de disco duro de las máquinas virtuales.

Objeto de intercambio de máquina virtual

Se crea cuando la máquina virtual está encendida.

VMDK delta de instantáneas

Se crean cuando se crean instantáneas de la máquina virtual. Estos discos delta no se crean para vSAN Express Storage Architecture.

Objeto de memoria

Se crea cuando está seleccionada la opción de memoria de instantánea al crear o suspender una máquina virtual.

Estado de conformidad de la máquina virtual: compatible y no compatible

Se considera que una máquina virtual está en estado de incumplimiento cuando uno de sus objetos o más no cumplen con los requisitos de la directiva de almacenamiento asignada. Por ejemplo, el estado puede pasar a ser de incumplimiento cuando no es posible acceder a una de las copias reflejadas. Si las máquinas virtuales cumplen con los requisitos definidos en la directiva de almacenamiento, el estado de las máquinas virtuales es de cumplimiento. Desde la

pestaña **Physical Disk Placement** (Ubicación de discos físicos) de la página **Virtual Disks** (Discos virtuales), puede comprobar el estado de conformidad de la máquina virtual. Para obtener información sobre la solución de problemas de un clúster de vSAN, consulte *Supervisar vSAN y solucionar sus problemas*.

Estado del componente: estados degradado y ausente

vSAN reconoce los siguientes estados de error para los componentes:

- Degraded (Degradado). Un componente entra en estado degradado cuando vSAN detecta un error permanente de un componente y determina que dicho componente no podrá recuperar su estado de funcionamiento original. En consecuencia, vSAN comienza a recompilar los componentes degradados de inmediato. Este estado puede producirse cuando un componente se encuentra en un dispositivo que genera un error.
- Absent (Ausente). Un componente entra en estado ausente cuando vSAN detecta un error temporal de un componente en el que el componente (incluidos todos sus datos) puede recuperarse y restaurar el estado original de vSAN. Este estado puede producirse cuando se reinician hosts o al desconectar un dispositivo de un host vSAN. vSAN espera 60 minutos antes de comenzar a recompilar los componentes en estado ausente.

Estado del objeto: correcto e incorrecto

Según el tipo y la cantidad de errores en el clúster, un objeto puede tener uno de los siguientes estados:

- Healthy (Estado correcto). Cuando hay disponible al menos un reflejo completo de RAID 1, o está disponible la cantidad mínima requerida de segmentos de datos, se considera que el objeto tiene un estado correcto.
- Unhealthy (Estado incorrecto). Se considera que un objeto tiene un estado incorrecto cuando no hay reflejos completos disponibles o el número mínimo requerido de segmentos de datos no está disponible para los objetos de RAID 5 o RAID 6. Si menos del 50 % de los votos de un objeto están disponibles, el objeto tiene un estado incorrecto. Varios errores en el clúster pueden provocar que los objetos entren en un estado incorrecto. Cuando un objeto tiene un estado operativo incorrecto, afecta la disponibilidad de la máquina virtual asociada.

Testigo

Un testigo es un componente que contiene únicamente metadatos y no datos reales de aplicaciones. Sirve como factor determinante cuando se debe tomar una decisión en relación con la disponibilidad de los componentes del almacén de datos restantes después de un error potencial. Un testigo utiliza aproximadamente 2 MB de espacio para metadatos en el almacén de datos de vSAN cuando se utiliza el formato en disco 1.0, y consume 4 MB para el formato en disco 2.0 y versiones posteriores.

vSAN mantiene quórum mediante un sistema de votación asimétrico en el que cada componente puede tener más de un voto para decidir la disponibilidad de los objetos. Para que un objeto se considere disponible, la accesibilidad de los votos que componen el objeto de almacenamiento de una máquina virtual debe ser superior al 50 % en todo momento. Cuando la cantidad de votos a los que todos los hosts pueden acceder es igual o inferior al 50 %, el almacén de datos de vSAN ya no puede acceder al objeto. Los objetos inaccesibles pueden afectar la disponibilidad de la máquina virtual asociada.

Administrar el almacenamiento basada en directivas (SPBM)

Al usar vSAN, puede definir requisitos de almacenamiento de máquinas virtuales, como el rendimiento y la disponibilidad, mediante una directiva. vSAN garantiza que a las máquinas virtuales implementadas en los almacenes de datos de vSAN se les asigne, al menos, una directiva de almacenamiento de máquinas virtuales. Cuando se conocen los requisitos de almacenamiento de las máquinas virtuales, es posible crear directivas de almacenamiento y asignar las directivas a las máquinas virtuales. Si no se aplica una directiva de almacenamiento al implementar las máquinas virtuales, vSAN asigna de manera automática una directiva predeterminada de vSAN con el atributo **Errores que se toleran** establecido en 1, una sola fracción de disco para cada objeto y un disco virtual con aprovisionamiento fino. Para obtener mejores resultados, defina sus propias directivas de almacenamiento de máquinas virtuales, aunque los requisitos de sus directivas sean iguales a los que se definen en la directiva de almacenamiento predeterminada. Para obtener información sobre el uso de directivas de almacenamiento de vSAN, consulte *Administrar VMware vSAN*.

vSphere PowerCLI

VMware vSphere PowerCLI incluye compatibilidad con scripts de línea de comandos para vSAN, que le ayudarán a automatizar las tareas de administración y configuración. vSphere PowerCLI proporciona una interfaz Windows PowerShell para vSphere API. PowerCLI incluye cmdlets para administrar los componentes de vSAN. Para obtener información sobre el uso de vSphere PowerCLI, consulte la *Documentación de vSphere PowerCLI*.

En qué se diferencia vSAN del almacenamiento tradicional

Aunque vSAN comparte muchas características con los arreglos de almacenamiento tradicionales, la función y el comportamiento general de vSAN son diferentes.

Por ejemplo, vSAN puede administrar y funcionar solo con hosts ESXi, y una instancia de vSAN proporciona un único almacén de datos para el clúster.

vSAN y el almacenamiento tradicional también se diferencian en los siguientes aspectos clave:

- vSAN no necesita almacenamiento en red externo para almacenar archivos de máquinas virtuales en una ubicación remota, por ejemplo, en una red de canal de fibra (Fibre Channel, FC) o en una red de área de almacenamiento (Storage Area Network, SAN).

- Con el almacenamiento tradicional, el administrador de almacenamiento asigna anticipadamente el espacio de almacenamiento en los distintos sistemas de almacenamiento. vSAN convierte de manera automática los recursos locales de almacenamiento físico de los hosts ESXi en un solo grupo de almacenamiento. Estos grupos pueden dividirse y asignarse a aplicaciones y máquinas virtuales en función de los requisitos de calidad de servicio.
- vSAN no se comporta como volúmenes de almacenamiento tradicionales basados en LUN o recursos compartidos NFS. El servicio del destino iSCSI usa LUN para habilitar un iniciador en un host remoto para transportar datos de nivel de bloque a un dispositivo de almacenamiento en el clúster de vSAN.
- Algunos protocolos de almacenamiento estándares, como FCP, no se aplican a vSAN.
- vSAN está altamente integrado con vSphere. A diferencia del almacenamiento tradicional, no se necesitan una consola de almacenamiento ni complementos dedicados para vSAN. Puede implementar, administrar y supervisar vSAN mediante vSphere Client.
- No se necesita un administrador de almacenamiento dedicado para administrar vSAN. En lugar de ello, un administrador de vSphere puede administrar un entorno de vSAN.
- Mediante vSAN, se asignan directivas de almacenamiento de máquina virtual de forma automática cuando se implementan nuevas máquinas virtuales. Es posible cambiar las directivas de almacenamiento de manera dinámica según sea necesario.

Compilar un clúster de vSAN

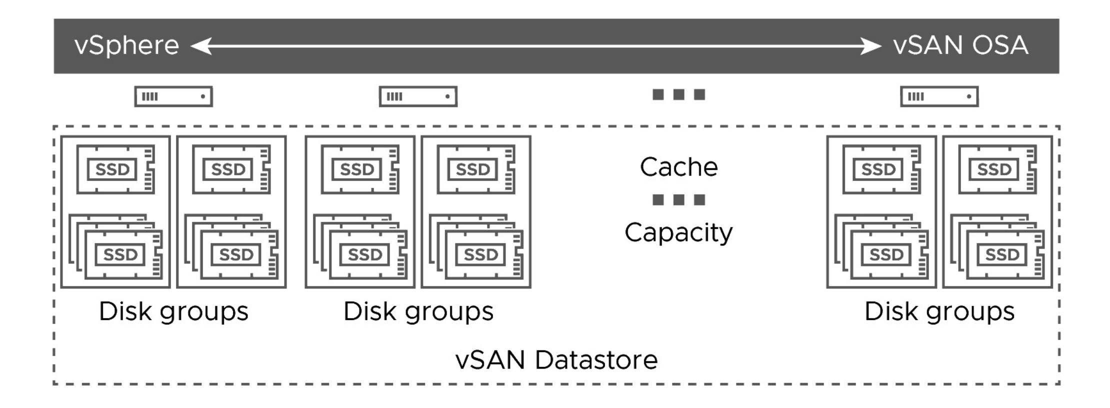
3

Puede elegir la arquitectura de almacenamiento y la opción de implementación al crear un clúster de vSAN.

Elija la arquitectura de almacenamiento vSAN que mejor se adapte a sus recursos y a sus necesidades.

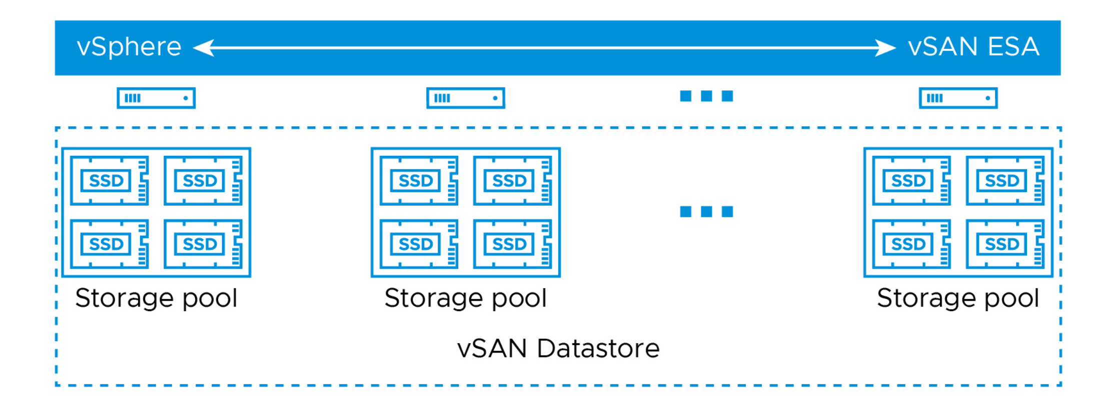
vSAN Original Storage Architecture

vSAN Original Storage Architecture (OSA) está diseñada para una amplia gama de dispositivos de almacenamiento, incluidas unidades flash de estado sólido (SSD) y unidades de disco magnético (HDD). Cada host que aporta almacenamiento contiene uno o varios grupos de discos. Cada grupo de discos contiene un dispositivo flash de almacenamiento en caché y uno o varios dispositivos de capacidad.



vSAN Express Storage Architecture

vSAN Express Storage Architecture (ESA) está diseñada para dispositivos flash TLC basados en NVMe y redes de alto rendimiento. Cada host que aporta almacenamiento contiene un solo grupo de almacenamiento de cuatro o más dispositivos flash. Cada dispositivo flash proporciona caché y capacidad al clúster.



Según sus requisitos, puede implementar vSAN de las siguientes formas:

vSAN ReadyNode

vSAN ReadyNode es una solución preconfigurada del software vSAN que proporcionan los partners de VMware, como Cisco, Dell, Fujitsu, IBM y Supermicro. Esta solución incluye configuración de servidores validada en un factor de forma de hardware probado y certificado para la implementación de vSAN que recomiendan el OEM del servidor y VMware. Para obtener información sobre la solución vSAN ReadyNode para un partner específico, visite el sitio web de partners de VMware.

Clúster de vSAN definido por el usuario

Puede compilar un clúster de vSAN seleccionando componentes de software y hardware individuales, como los controladores, el firmware y los controladores de E/S de almacenamiento que se enumeran en el sitio web de la guía de compatibilidad de vSAN (vSAN Compatibility Guide, VCG), en la siguiente URL: http://www.vmware.com/resources/compatibility/search.php. Puede elegir cualquier tipo de servidores, controladores de E/S de almacenamiento, dispositivos de capacidad y dispositivos flash de almacenamiento en caché y memoria, y cualquier cantidad de núcleos que necesite por CPU, que se certifiquen y se enumeren en el sitio web de VCG. Consulte la información de compatibilidad del sitio web de VCG antes de elegir los componentes de software y hardware, los controladores, el firmware y los controladores de E/S de almacenamiento compatibles con vSAN. Al diseñar un clúster de vSAN, use únicamente dispositivos, firmware y controladores que se enumeren en el sitio web de VCG. El uso de versiones de software y hardware no enumeradas en VCG puede ocasionar un error del clúster o una pérdida de datos inesperada. Para obtener información sobre el diseño de un clúster de vSAN, consulte "Diseñar y dimensionar un clúster de vSAN" en *Planificar e implementar vSAN*.

Lea los siguientes temas a continuación:

- Opciones de implementación de vSAN

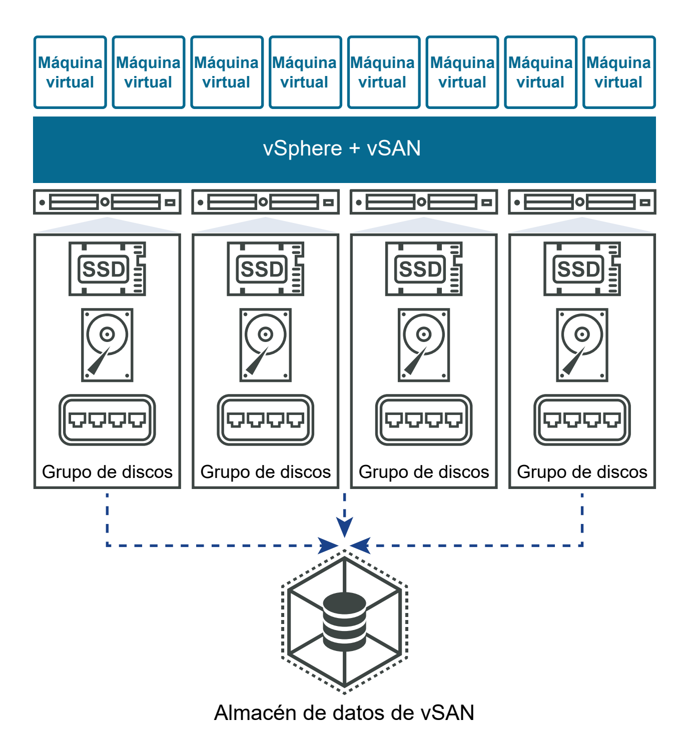
Opciones de implementación de vSAN

En esta sección se tratan las opciones de implementación compatibles con los clústeres de vSAN.

Clúster de vSAN de sitio único

Un clúster de vSAN de sitio único consta de un mínimo de tres hosts. Por lo general, todos los hosts de un clúster de vSAN de sitio único se encuentran en una misma ubicación y están conectados en la misma red de capa 2. Las configuraciones basadas íntegramente en tecnología flash requieren conexiones de red de 10 Gb, y vSAN Express Storage Architecture requiere conexiones de red de 25 Gb.

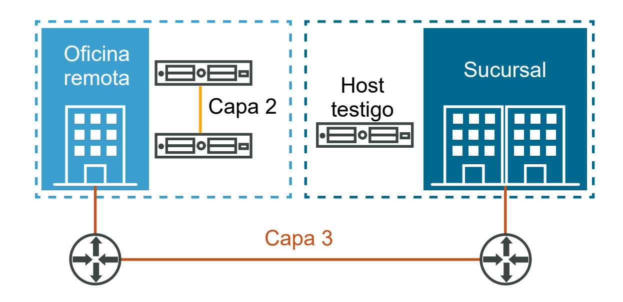
Para obtener más información, consulte Crear un clúster de vSAN de sitio único.



Clúster de vSAN de dos nodos

A menudo se utilizan clústeres de vSAN de dos nodos para entornos de oficina remota o sucursales donde, por lo general, se ejecuta una pequeña cantidad de cargas de trabajo que requieren alta disponibilidad. Un clúster de vSAN de dos nodos consta de dos hosts en la misma ubicación, conectados al mismo conmutador de red o conectados directamente. Puede configurar un clúster de vSAN de dos nodos que utilice un tercer host como testigo, el cual puede estar ubicado remotamente respecto de la sucursal. El testigo suele residir en el sitio principal, junto con vCenter Server.

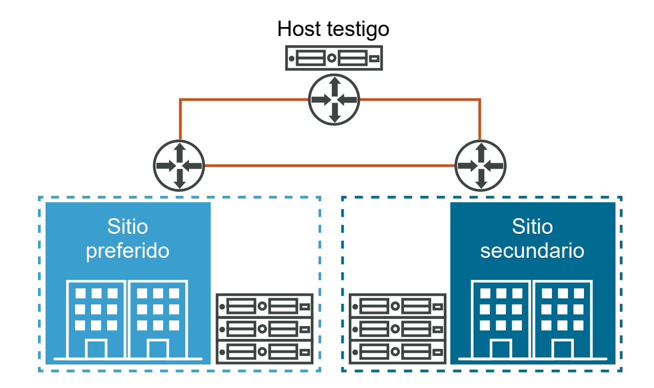
Para obtener más información, consulte Crear un clúster de vSAN ampliado o de dos nodos.



Clúster ampliado de vSAN

Un clúster ampliado de vSAN proporciona resistencia contra la pérdida de un sitio entero. Los hosts de un clúster ampliado de vSAN se distribuyen uniformemente entre dos sitios. Los dos sitios deben tener una latencia de red de no más de 5 milisegundos (5 ms). Un host testigo de vSAN se encuentra en un tercer sitio para cumplir la función de testigo. El testigo también permite desempatar en los escenarios en los que se produce una partición de red entre los dos sitios de datos. En el testigo, solamente se almacenan metadatos como componentes testigo.

Para obtener más información, consulte Crear un clúster de vSAN ampliado o de dos nodos.



Integrar vSAN con otro software de VMware

4

Una vez que vSAN está activo y en funcionamiento, se integra con el resto de la pila de software de VMware.

Puede hacer la mayoría de las cosas que con el almacenamiento tradicional utilizando componentes y características de vSphere, que incluyen vSphere vMotion, instantáneas, clones, Distributed Resource Scheduler (DRS), vSphere High Availability, VMware Site Recovery Manager y más.

vSphere HA

Puede habilitar vSphere HA y vSAN en el mismo clúster. Al igual que con los almacenes de datos tradicionales, vSphere HA proporciona el mismo nivel de protección para las máquinas virtuales en los almacenes de datos de vSAN. El nivel de protección impone restricciones específicas cuando interactúan vSphere HA y vSAN . Para conocer consideraciones específicas sobre la integración de vSphere HA y vSAN, consulte "Usar vSAN y vSphere HA" en *Planificar e implementar vSAN*.

VMware Horizon View

Puede integrar vSAN con VMware Horizon View. Cuando se integra, vSAN proporciona los siguientes beneficios a los entornos de escritorios virtuales:

- Almacenamiento de alto rendimiento con almacenamiento en caché automático
- Administración de almacenamiento basada en directivas, para corrección automática

Para obtener información sobre la integración de vSAN con VMware Horizon, consulte la documentación de *VMware con Horizon View*. Si desea información sobre el diseño y el dimensionamiento de VMware Horizon View para vSAN, consulte la *guía de diseño y dimensionamiento para Horizon View*.

Limitaciones de vSAN

5

En este tema se analizan las limitaciones de vSAN.

Al trabajar con vSAN, tenga en cuenta las siguientes limitaciones:

- vSAN no admite hosts que participen en varios clústeres de vSAN. Sin embargo, un host de vSAN puede acceder a otros recursos de almacenamiento externo que se comparten entre todos los clústeres.
- vSAN no admite vSphere DPM ni Storage I/O Control.
- vSAN no admite discos SE dispersos.
- vSAN no admite RDM, VMFS, partición de diagnóstico ni otras características de acceso a dispositivos.

Configurar y administrar un clúster de vSAN

6

Puede configurar y administrar un clúster de vSAN mediante vSphere Client, los comandos esxcli y otras herramientas.

Lea los siguientes temas a continuación:

Configurar un clúster de vSAN mediante vSphere Client

Puede utilizar vSphere Client para configurar vSAN en un clúster existente.

Nota Puede utilizar el inicio rápido para crear y configurar un clúster de vSAN rápidamente. Para obtener más información, consulte "Usar el inicio rápido para configurar y expandir un clúster de vSAN" en *Planificar e implementar vSAN*.

Requisitos previos

Compruebe que el entorno cumpla con todos los requisitos. Consulte "Requisitos para habilitar vSAN" en *Implementación y planificación de vSAN*.

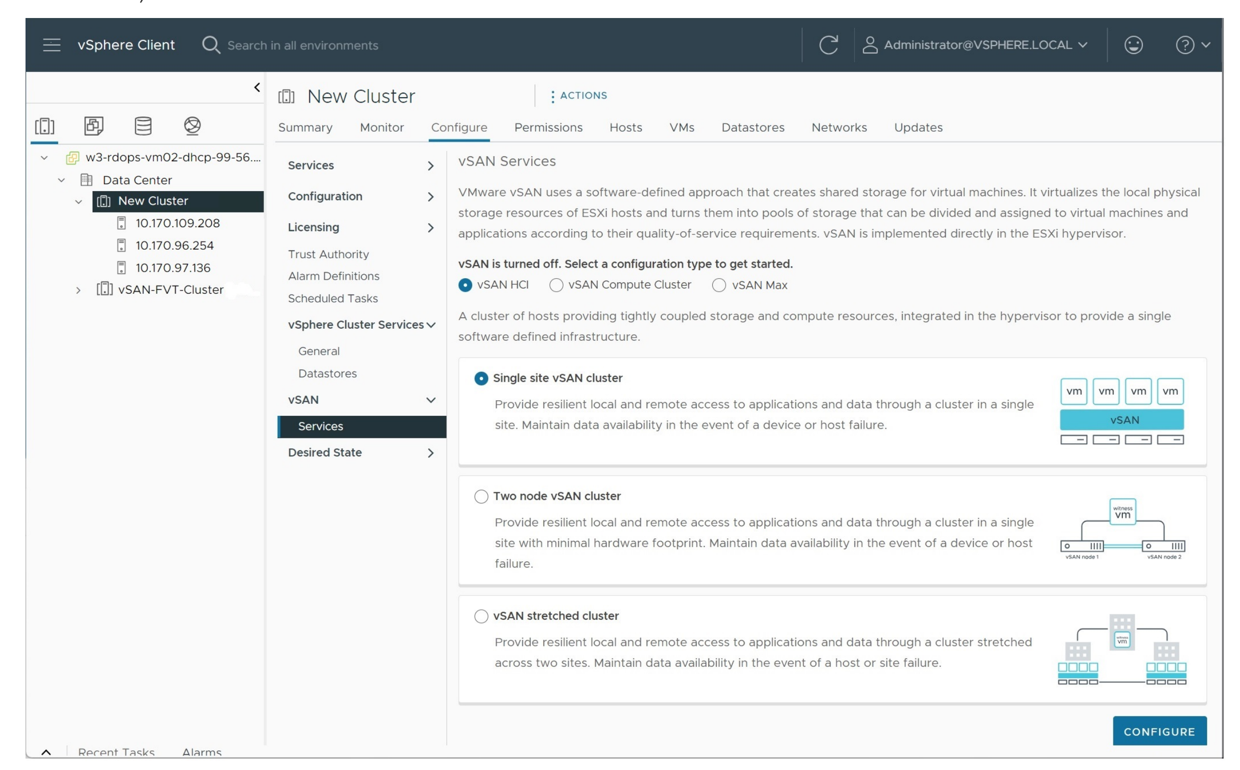
Cree un clúster y agregue hosts al clúster antes de habilitar y configurar vSAN. Configure las propiedades del puerto en cada host para agregar el servicio de vSAN.

Procedimiento

1 Desplácese hasta un clúster de host.

2 Haga clic en la pestaña **Configurar**.

3 En vSAN, seleccione **Servicios**.



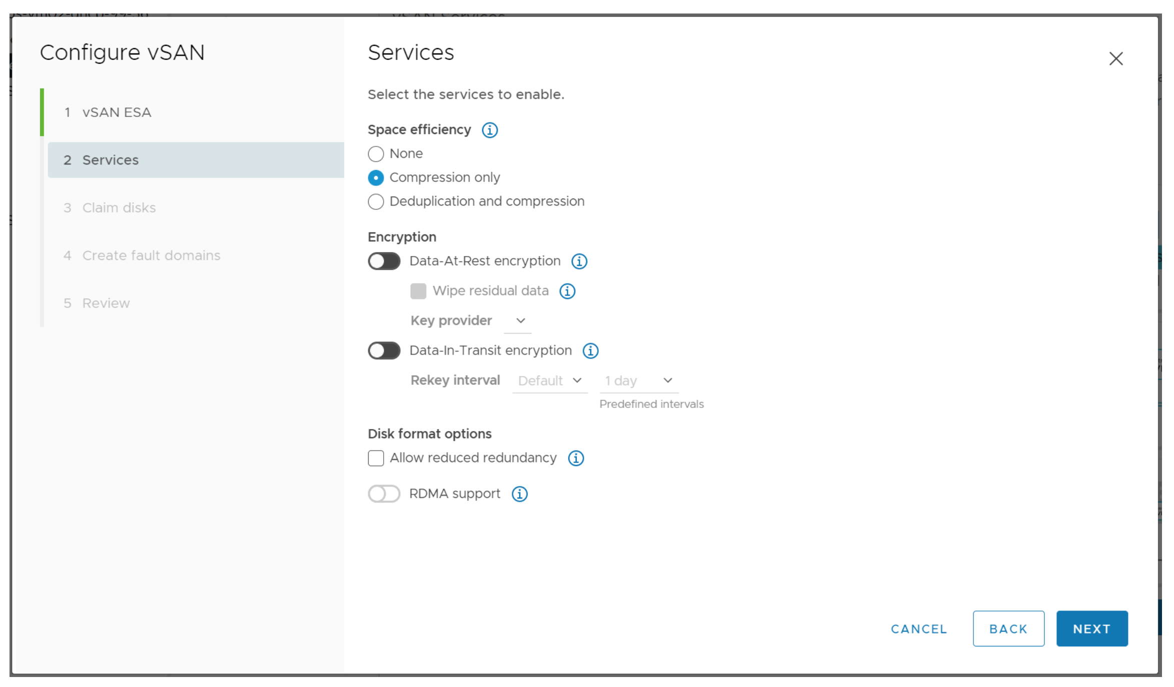
a Seleccione un tipo de configuración de HCI.

- **vSAN HCI** proporciona recursos informáticos y de almacenamiento. El almacén de datos se puede compartir entre clústeres del mismo centro de datos y entre clústeres administrados por instancias remotas de vCenter.
- **Clúster de proceso de vSAN** solo proporciona recursos informáticos de vSphere. Puede montar almacenes de datos servidos por clústeres de vSAN Max en el mismo centro de datos y desde instancias remotas de vCenter.

- **vSAN Max** (clústeres de vSAN ESA) proporciona recursos de almacenamiento, pero no recursos informáticos. El almacén de datos se puede montar mediante clústeres de vSphere cliente y clústeres de vSAN en el mismo centro de datos y desde instancias remotas de vCenter.

b Seleccione una opción de implementación (Clúster de vSAN de sitio único, Clúster de vSAN de dos nodos o Clúster ampliado de vSAN).

c Haga clic en **Configurar** para abrir el asistente de configuración de vSAN.



4 Seleccione vSAN ESA si el clúster es compatible y haga clic en **Siguiente**.

5 Configure los servicios de vSAN que desea utilizar y haga clic en **Siguiente**.

Configure las funciones de administración de datos, como la desduplicación y la compresión, el cifrado de datos en reposo y el cifrado de datos en tránsito. Seleccione RDMA (acceso directo remoto a la memoria) si la red lo admite.

6 Reclame discos para el clúster de vSAN y haga clic en **Siguiente**.

Para vSAN Original Storage Architecture (vSAN OSA), cada host que aporte almacenamiento requiere al menos un dispositivo flash para memoria caché y uno o varios dispositivos para capacidad. Para vSAN Express Storage Architecture (vSAN ESA), cada host que aporta almacenamiento requiere uno o varios dispositivos flash.

7 Cree dominios de errores para hosts que se puedan producir errores en conjunto.

8 Revise la configuración y haga clic en **Finalizar**.

Resultados

Al habilitar vSAN, se crea un almacén de datos de vSAN y se registra el proveedor de almacenamiento de vSAN. Los proveedores de almacenamiento de vSAN son componentes

de software integrados que comunican las funcionalidades de almacenamiento del almacén de datos a vCenter Server.

Pasos siguientes

Compruebe que se haya creado el almacén de datos de vSAN. Consulte Ver el almacén de datos de vSAN.

Compruebe que el proveedor de almacenamiento de vSAN esté registrado.

Habilitar vSAN en un clúster existente

Puede habilitar vSAN en un clúster existente, así como configurar funciones y servicios.

Requisitos previos

Compruebe que el entorno cumpla con todos los requisitos. Consulte "Requisitos para habilitar vSAN" en *Implementación y planificación de vSAN*.

Procedimiento

1. Desplácese hasta un clúster de host.
2. Haga clic en la pestaña **Configurar**.
3. En vSAN, seleccione **Servicios**.
   a. Seleccione un tipo de configuración (Clúster de vSAN de sitio único, Clúster de vSAN de dos nodos o Clúster ampliado de vSAN).
   b. Seleccione **Necesito un almacén de datos de vSAN local** si tiene pensado agregar grupos de discos o grupos de almacenamiento a los hosts del clúster.
   c. Haga clic en **Configurar** para abrir el asistente de configuración de vSAN.
4. Seleccione vSAN ESA si el clúster es compatible y haga clic en **Siguiente**.
5. Configure los servicios de vSAN que desea utilizar y haga clic en **Siguiente**.

   Configure las funciones de administración de datos, como la desduplicación y la compresión, el cifrado de datos en reposo y el cifrado de datos en tránsito. Seleccione RDMA (acceso directo remoto a la memoria) si la red lo admite.
6. Reclame discos para el clúster de vSAN y haga clic en **Siguiente**.

   Para vSAN Original Storage Architecture (vSAN OSA), cada host que aporte almacenamiento requiere al menos un dispositivo flash para memoria caché y uno o varios dispositivos para capacidad. Para vSAN Express Storage Architecture (vSAN ESA), cada host que aporta almacenamiento requiere uno o varios dispositivos flash.
7. Cree dominios de errores para hosts que se puedan producir errores en conjunto.
8. Revise la configuración y haga clic en **Finalizar**.

Desactivar vSAN

Puede desactivar vSAN para un clúster de host.

Cuando se desactiva vSAN en un clúster, todas las máquinas virtuales y los servicios de datos ubicados en el almacén de datos de vSAN dejan de estar accesibles. Si consumió almacenamiento en el clúster de vSAN mediante vSAN Direct, los servicios de supervisión de vSAN Direct, como las comprobaciones de estado, los informes de espacio y la supervisión del rendimiento, no estarán disponibles. Si va a usar máquinas virtuales mientras vSAN está desactivado, asegúrese de migrar las máquinas virtuales del almacén de datos de vSAN a otro almacén de datos antes de desactivar el clúster de vSAN.

Requisitos previos

Compruebe que los hosts estén en modo de mantenimiento. Para obtener más información, consulte Poner un miembro de un clúster de vSAN en modo de mantenimiento.

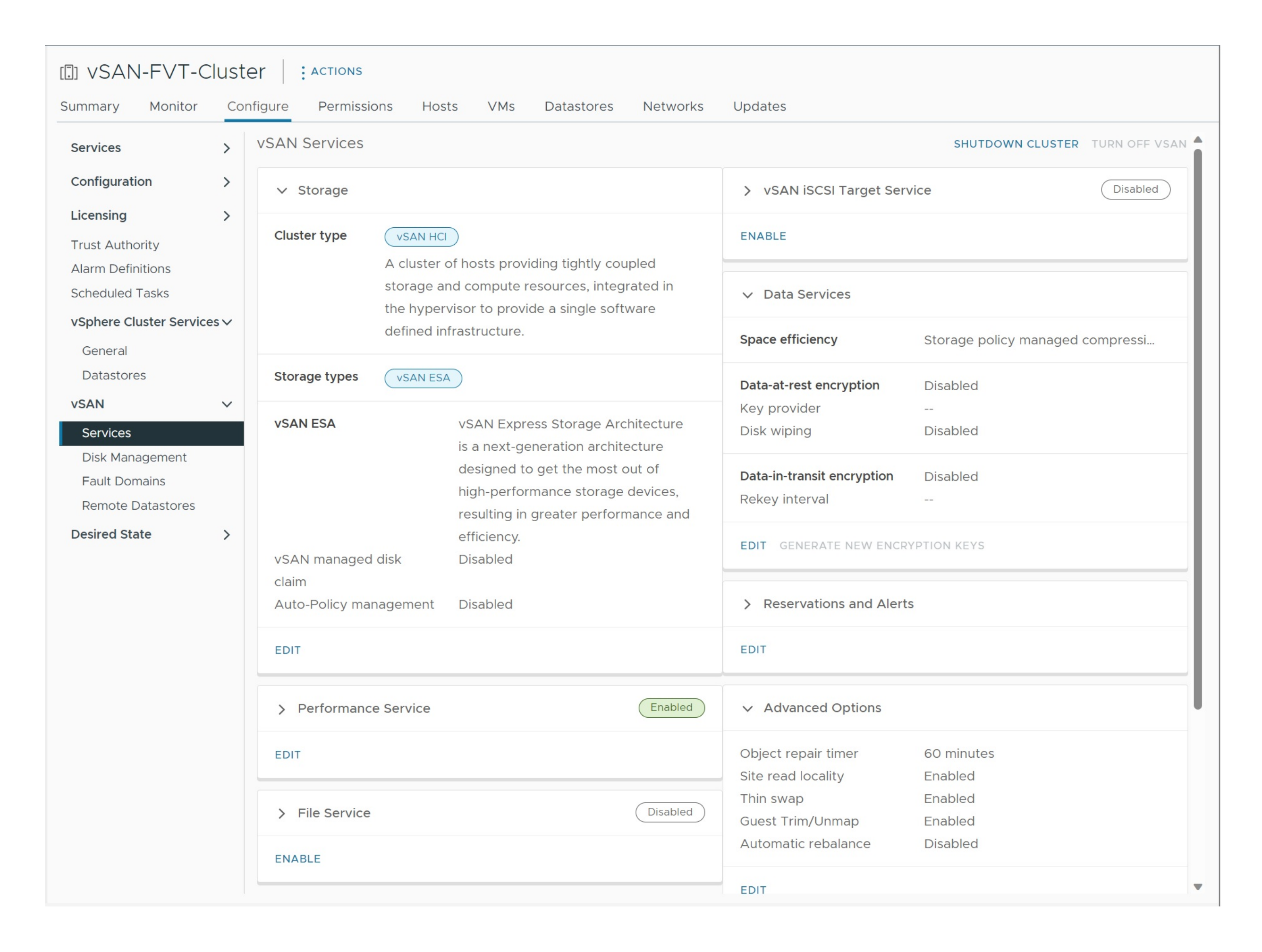
Procedimiento

1 Desplácese hasta el clúster de vSAN.
2 Haga clic en la pestaña **Configurar**.
3 En vSAN, seleccione **Servicios**.
4 Haga clic en **Desactivar vSAN**.
5 En el cuadro de diálogo Desactivar vSAN, confirme la selección.

Editar la configuración de vSAN

Puede editar la configuración del clúster de vSAN para configurar las funciones de administración de datos y habilitar los servicios proporcionados por el clúster.

Edite la configuración de un clúster de vSAN existente si desea habilitar la desduplicación y la compresión, o para cambiar el método de cifrado. Si habilita la desduplicación y la compresión, o el cifrado, el formato en disco del clúster se actualiza automáticamente a la versión más reciente.



Procedimiento

1 Desplácese hasta el clúster de vSAN.

2 Haga clic en la pestaña **Configurar**.

   a En vSAN, seleccione **Servicios**.

   b Haga clic en el botón **Editar** o **Habilitar** correspondiente al servicio que desee configurar.

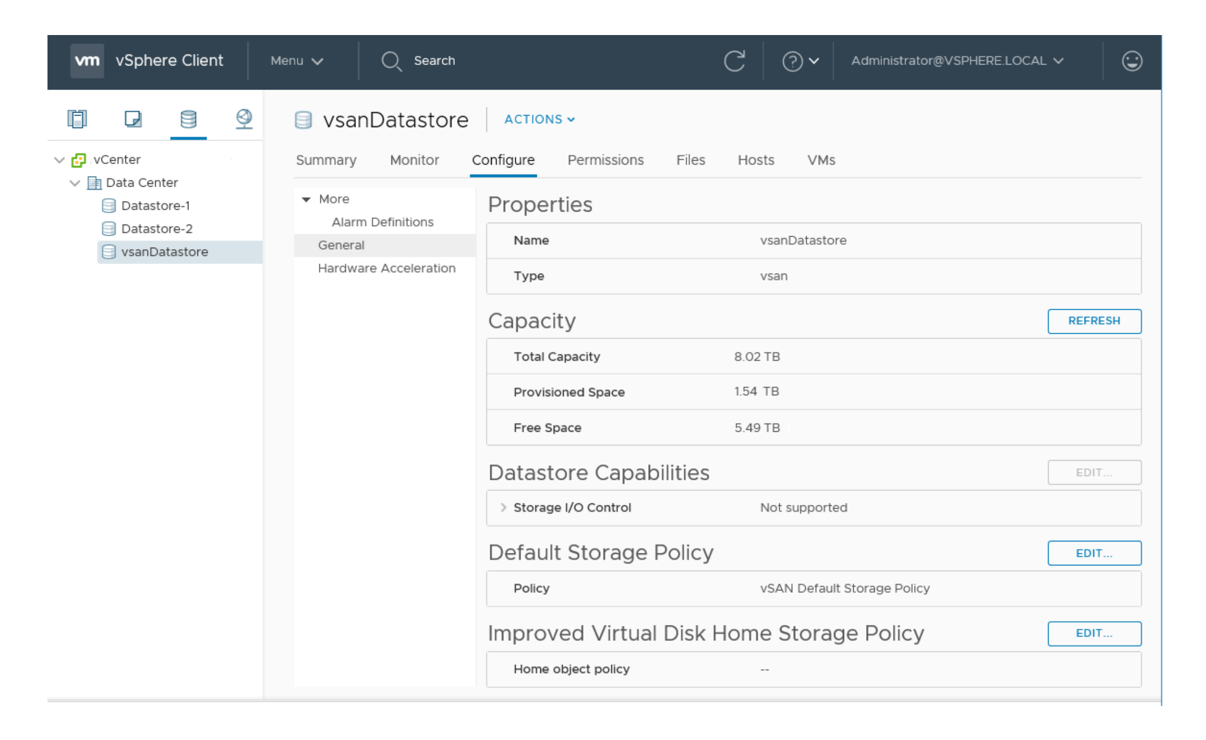
      - Configurar almacenamiento. Haga clic en **Montar almacenes de datos remotos** para usar el almacenamiento de otros clústeres de vSAN.
      - Configure el servicio de rendimiento de vSAN. Para obtener más información, consulte "Supervisar el rendimiento de vSAN" en *Supervisar vSAN y solucionar sus problemas*.
      - Habilitar el servicio de archivos. Para obtener más información, consulte "Servicio de archivos de vSAN" en *Administrar VMware vSAN*.
      - Configure las opciones de red de vSAN. Para obtener más información, consulte "Configurar la red de vSAN" en *Planificar e implementar vSAN*.
      - Configure el servicio del destino iSCSI. Para obtener más información, consulte "Uso del servicio del destino iSCSI de vSAN" en *Administrar VMware vSAN*.
      - Configure los servicios de datos, como la desduplicación y la compresión, el cifrado de datos en reposo y el cifrado de datos en tránsito.
      - Configure vSAN Data Protection. Antes de utilizar vSAN Data Protection, debe implementar el servicio de instantáneas de vSAN. Para obtener más información, consulte "Implementación del dispositivo del servicio de instantáneas" en *Administrar VMware vSAN*.
      - Configure alertas y reservas de capacidad. Para obtener más información, consulte "Acerca de la capacidad reservada" en *Supervisar vSAN y solucionar sus problemas*.
      - Configure las opciones avanzadas:
        - Temporizador de reparación de objetos
        - Ubicación de lectura de sitios para clústeres ampliados de vSAN
        - Aprovisionamiento de intercambio fino
        - Compatibilidad con clústeres grandes para hasta 64 hosts
        - Reequilibrio automático
      - Configure el servicio de estado histórico de vSAN.

   c Modifique la configuración para que coincida con sus requisitos.

3 Haga clic en **Aplicar** para confirmar sus selecciones.

Ver el almacén de datos de vSAN

Después de activar vSAN, se crea un solo almacén de datos. Puede revisar la capacidad del almacén de datos de vSAN.



Requisitos previos

Configure vSAN y grupos de discos o grupos de almacenamiento.

Procedimiento

1 Desplácese hasta el almacenamiento.

2 Seleccione el almacén de datos de vSAN.

3 Haga clic en la pestaña **Configurar**.

4 Revise la capacidad del almacén de datos de vSAN.

   El tamaño del almacén de datos de vSAN depende de la cantidad de dispositivos de capacidad por cada host ESXi de la cantidad de hosts ESXi en el clúster. Por ejemplo, si un host cuenta con 7 dispositivos de capacidad de 2 TB y el clúster incluye 8 hosts, la capacidad de almacenamiento aproximada es la siguiente: 7 x 2 TB x 8 = 112 TB. Al usar la configuración basada íntegramente en tecnología flash, se utilizan dispositivos flash para la capacidad. Para las configuraciones híbridas, se utilizan discos magnéticos para la capacidad.

   Algo de capacidad se asigna para los metadatos.

   - El formato en disco versión 1.0 agrega aproximadamente 1 GB por dispositivo de capacidad.
   - El formato en disco versión 2.0 agrega una sobrecarga de capacidad, que generalmente no excede el 1-2 % de capacidad por dispositivo.

- El formato en disco versión 3.0 y posteriores agrega una sobrecarga de capacidad, que generalmente no excede el 1-2 % de capacidad por dispositivo. La desduplicación y la compresión con la suma de comprobación de software habilitada requieren una sobrecarga adicional de aproximadamente 6,2 % de capacidad por dispositivo.

Pasos siguientes

Cree una directiva de almacenamiento para máquinas virtuales con las capacidades de almacenamiento del almacén de datos de vSAN. Para obtener información, consulte el documento *Almacenamiento de vSphere*.

Cargar archivos o carpetas en almacenes de datos de vSAN

Puede cargar archivos VMDK en un almacén de datos de vSAN.

También puede cargar carpetas en un almacén de datos de vSAN. Para obtener más información sobre los almacenes de datos, consulte *Almacenamiento de vSphere*. Para la carga de un archivo VMDK en un almacén de datos de vSAN, rigen las siguientes consideraciones:

- Solo puede cargar archivos VMDK optimizados para transmisión en un almacén de datos de vSAN. El formato de archivo optimizado para secuencias de VMware es un formato monolítico disperso comprimido para la transmisión por secuencias. Si el archivo VMDK no está en formato optimizado para transmisión, antes de cargarlo, conviértalo a dicho formato mediante la utilidad vmware-vdiskmanager command-line. Para obtener más información, consulte la *Guía de usuario del administrador de disco virtual*.
- Cuando se carga un archivo VMDK en un almacén de datos de vSAN, el archivo hereda la directiva predeterminada de ese almacén de datos. Por lo tanto, el archivo VMDK no hereda la directiva de la máquina virtual desde la que se descargó. vSAN crea los objetos aplicando la directiva predeterminada vsanDatastore, que es RAID-1. Puede cambiar la directiva predeterminada del almacén de datos. Consulte Cambiar la directiva de almacenamiento predeterminada de los almacenes de datos de vSAN .
- El archivo VMDK debe cargarse en la carpeta de inicio de la máquina virtual.

Procedimiento

1 Desplácese al almacén de datos de vSAN.

2 Haga clic en la pestaña **Archivos**.

Opción	Descripción
Cargar archivos	a Seleccione la carpeta de destino y haga clic en **Cargar archivos**. Verá un mensaje donde se le informa de que solo puede cargar archivos VMDK en el formato optimizado para transmisión de VMware. Si intenta cargar un archivo VMDK en un formato diferente, verá un mensaje de error interno del servidor. b Haga clic en **Cargar**. c Busque el elemento que desea cargar en el equipo local y haga clic en **Abrir**.
Cargar carpetas	a Seleccione la carpeta de destino y haga clic en **Cargar carpeta**. Verá un mensaje donde se le informa de que solo puede cargar archivos VMDK en el formato optimizado para transmisión de VMware. b Haga clic en **Cargar**. c Busque el elemento que desea cargar en el equipo local y haga clic en **Abrir**.

Descargar archivos o carpetas de almacenes de datos de vSAN

Puede descargar archivos y carpetas de un almacén de datos de vSAN.

Para obtener más información sobre los almacenes de datos, consulte *Almacenamiento de vSphere*. Los archivos vmdk se descargan como archivos optimizados para secuencias con el nombre de archivo `<vmdkName>_stream.vmdk`. El formato de archivo optimizado para secuencias de VMware es un formato monolítico disperso comprimido para la transmisión por secuencias.

Puede convertir un archivo vmdk optimizado para secuencias de VMware a otros formatos de archivo vmdk mediante la utilidad de línea de comandos vmware-vdiskmanager. Para obtener más información, consulte la *Guía de usuario del administrador de disco virtual*.

Procedimiento

1 Desplácese al almacén de datos de vSAN.

2 Haga clic en la pestaña **Archivos** y, a continuación, en **Descargar**.

   Verá un mensaje donde se advierte que los archivos vmdk se descargarán de los almacenes de datos de vSAN en el formato optimizado para secuencias de VMware con la extensión de nombre de archivo `.stream.vmdk`.

3 Haga clic en **Descargar**.

4 Busque el elemento que desea descargar y, a continuación, haga clic en **Descargar**.

Usar las directivas de vSAN

7

Al usar vSAN, puede definir requisitos de almacenamiento de máquinas virtuales, como el rendimiento y la disponibilidad, mediante una directiva.

vSAN garantiza que a cada máquina virtual implementada en los almacenes de datos de vSAN se le asigne, al menos, una directiva de almacenamiento. Una vez asignados, los requisitos de la directiva de almacenamiento se traspasan a la capa de vSAN cuando se crea una máquina virtual. El dispositivo virtual se distribuye en el almacén de datos de vSAN para cumplir con los requisitos de rendimiento y disponibilidad.

vSAN utiliza proveedores de almacenamiento para suministrar información sobre el almacenamiento subyacente a vCenter Server. Esta información ayuda a tomar las decisiones adecuadas sobre la selección de máquinas virtuales y a supervisar el entorno de almacenamiento.

Lea los siguientes temas a continuación:

¿Qué son las directivas de vSAN?

Las directivas de almacenamiento de vSAN definen los requisitos de almacenamiento para las máquinas virtuales.

Estas directivas determinan cómo los objetos de almacenamiento de máquinas virtuales se aprovisionan y asignan dentro del almacén de datos para garantizar el nivel de servicio requerido. Al habilitar vSAN en un clúster del host, se crea un solo almacén de datos de vSAN y, asimismo, se asigna una directiva de almacenamiento predeterminada al almacén de datos.

Cuando se conocen los requisitos de almacenamiento de las máquinas virtuales, es posible crear una directiva de almacenamiento que hace referencia a las funcionalidades que anuncia el almacén de datos. Puede crear varias directivas para capturar distintos tipos o distintas clases de requisitos.

Se asigna a cada máquina virtual implementada en los almacenes de datos de vSAN al menos una directiva de almacenamiento de máquinas virtuales. Puede asignar estas directivas de almacenamiento al crear o editar máquinas virtuales.

Nota Si no asigna una directiva de almacenamiento a una máquina virtual, vSAN asigna una directiva predeterminada. La directiva predeterminada tiene la opción **Errores que se toleran** configurada en 1, una sola fracción de disco por objeto y un disco virtual con aprovisionamiento fino.

El objeto de intercambio de máquina virtual y el objeto de memoria de instantánea de máquina virtual cumplen con las directivas de almacenamiento asignadas a una máquina virtual, con **Errores que se toleran** configurado con el valor 1. Es posible que su disponibilidad no sea igual a la de otros objetos que tengan asignada una directiva con un valor diferente para **Errores que se toleran**.

Nota Si se habilita vSAN Express Storage Architecture, cada instantánea no se considerará un objeto nuevo. Los VMDK base y sus instantáneas estarán contenidos en un objeto de vSAN. Además, en vSAN ESA, el resumen estará respaldado por el objeto de vSAN. Esto es diferente de vSAN Original Storage Architecture.

Tabla 7-1. Directiva de almacenamiento: Disponibilidad

Funcionalidad	Descripción
Errores que se toleran (FTT)	Define el número de errores de dispositivos y hosts que se pueden tolerar en un objeto de una máquina virtual. Para errores `n` tolerados, cada dato escrito se almacena en las ubicaciones `n+1`, incluidas las copias de paridad si se utiliza RAID-5 o RAID-6. Si se configuran dominios de errores, se requieren `2n+1` dominios de errores con hosts que aporten capacidad. Un host que no forma parte de ningún dominio de errores se considera su propio dominio de errores de host individual. Puede seleccionar un método de replicación de datos que optimice el rendimiento o la capacidad. RAID-1 (creación de reflejos) utiliza más espacio de disco para colocar los componentes de los objetos, pero proporciona un mejor rendimiento para acceder a los objetos. RAID-5/6 (codificación de borrado) utiliza menos espacio de disco, pero se reduce el rendimiento. Puede seleccionar una de las siguientes opciones: ■ **Sin redundancia de datos**: especifique esta opción si no desea que vSAN proteja una única copia reflejada de los objetos de máquina virtual. Eso significa que los datos quedan desprotegidos y se pueden perder cuando el clúster de vSAN detecta un error del dispositivo. Es posible que el host experimente demoras inusuales al entrar en el modo de mantenimiento. Los retrasos ocurren porque vSAN debe evacuar el objeto del host para que la operación de mantenimiento se complete correctamente. ■ **Sin redundancia de datos con afinidad de host** : especifique esta opción solo si desea ejecutar cargas de trabajo de vSAN Shared Nothing Architecture (SNA) en la plataforma de persistencia de datos de vSAN. ■ **1 error - RAID-1 (creación de reflejo)**: especifique esta opción si el objeto de máquina virtual puede tolerar un error de host o de dispositivo. Para proteger un objeto de máquina virtual de 100 GB mediante RAID-1 (creación de reflejo) con un FTT de 1, se consumirán 200 GB. ■ **1 error - RAID-5 (codificación de borrado)**: especifique esta opción si el objeto de máquina virtual puede tolerar un error de host o de dispositivo. En vSAN OSA, para proteger un objeto de máquina virtual de 100 GB mediante RAID-5 (codificación de borrado) con un FTT de 1, se consumirán 133,33 GB. **Nota** Si utiliza vSAN Express Storage Architecture, vSAN creará un formato RAID-5 optimizado en función del tamaño del clúster. Si el número de hosts del clúster es inferior a 6, vSAN creará un formato RAID-5 (2+1). Si el número de hosts es superior a 6, vSAN creará un formato RAID-6 (4+1). Cuando el tamaño del clúster finalmente se expande o se reduce, vSAN reajustará automáticamente el formato después de 24 horas desde el cambio de configuración. ■ **2 errores - RAID-1 (creación de reflejo)**: especifique esta opción si el objeto de máquina virtual puede tolerar hasta dos errores de dispositivo. Dado que necesita tener un FTT de 2 que use RAID-1 (creación de reflejo), se produce una sobrecarga de capacidad. Para proteger un objeto de máquina virtual de 100 GB mediante RAID-1 (creación de reflejo) con un FTT de 2, se consumirán 300 GB.

Tabla 7-1. Directiva de almacenamiento: Disponibilidad (continuación)

Funcionalidad	Descripción
	■ **2 errores - RAID-6 (codificación de borrado)**: especifique esta opción si los objetos de máquina virtual pueden tolerar hasta dos errores de dispositivo. Para proteger un objeto de máquina virtual de 100 GB mediante RAID-6 (codificación de borrado) con un FTT de 2, se consumirán 150 GB. Para obtener más información, consulte Usar la codificación de borrado RAID 5 o RAID 6 en un clúster de vSAN. ■ **3 errores - RAID-1 (creación de reflejo)**: especifique esta opción si los objetos de la máquina virtual pueden tolerar hasta tres errores de dispositivo. Para proteger un objeto de máquina virtual de 100 GB mediante RAID-1 (creación de reflejo) con un FTT de 3, se consumirán 400 GB. **Nota** Si se crea una directiva de almacenamiento y no se especifica un valor para **FTT**, vSAN crea una sola copia reflejada de los objetos de máquina virtual. Puede tolerar un solo error. Sin embargo, si ocurren varios errores de componentes, los datos podrían estar en riesgo.
Tolerancia ante desastres del sitio	Esta regla define si se debe utilizar un clúster estándar, ampliado o de 2 nodos. Si utiliza un clúster ampliado de vSAN, puede definir si los datos se reflejarán en ambos sitios o solo en uno. Para un clúster ampliado de vSAN, puede elegir mantener los datos en el sitio preferido o secundario para la afinidad de host. ■ **Ninguno: clúster estándar** es el valor predeterminado. Eso significa que no habrá tolerancia ante desastres en el sitio. ■ **Creación de reflejo del host: clúster de 2 nodos** define el número de errores adicionales que puede tolerar un objeto después de alcanzar el número de errores definidos por FTT. vSAN realiza la creación de reflejo del objeto en el nivel del grupo de discos. Cada host de datos debe tener al menos tres grupos de discos o tres discos en un grupo de almacenamiento para utilizar esta regla. ■ **Creación de reflejo de sitio: clúster ampliado** define el número de errores de host adicionales que puede tolerar el objeto después de alcanzar el número de errores de sitios definido por FTT. ■ **Ninguno: mantiene los datos en Preferido (clúster ampliado)**. Utilice esta opción si no desea que los objetos de un clúster ampliado de vSAN tengan tolerancia a errores en sitios y desea que los objetos sean accesibles solo en el sitio que está configurado como Preferido. ■ **Ninguno: mantiene los datos en Secundario (clúster ampliado)**. Utilice esta opción si no desea que los objetos de un clúster ampliado de vSAN tengan tolerancia a errores en sitios y desea que los objetos sean accesibles solo en el sitio secundario. Estos objetos no se ven afectados por errores del host testigo o el vínculo entre conmutadores (ISL). Permanecen accesibles si se puede acceder al sitio elegido por la directiva. ■ **Ninguno: clúster ampliado**. Si selecciona esta opción, vSAN no garantiza que se pueda acceder a los objetos si uno de los sitios falla, y dichos objetos podrían consumir demasiado ancho de banda de ISL y aumentar la latencia de los objetos que utilizan la directiva

Tabla 7-1. Directiva de almacenamiento: Disponibilidad (continuación)

Funcionalidad	Descripción
	de creación de reflejo del sitio. Use esta directiva solo cuando no pueda usar las otras durante alguna condición temporal en la que haya una restricción de capacidad (CPU/memoria/almacenamiento) en el clúster.

Tabla 7-2. Directiva de almacenamiento: reglas de almacenamiento

Funcionalidad	Descripción
Servicios de cifrado	Define las opciones de cifrado para las máquinas virtuales que se implementan en el almacén de datos. Seleccione una de las siguientes opciones: ■ **Cifrado de datos en reposo**: especifique esta opción si desea aplicar el cifrado a los datos almacenados en el almacén de datos. ■ **Sin cifrado**: especifique esta opción si no desea aplicar ningún tipo de cifrado a los datos. ■ **Sin preferencia**: especifique esta opción si no desea aplicar explícitamente ninguna regla de cifrado. Al seleccionar esta opción, vSAN aplicará ambas reglas a las máquinas virtuales.
Eficiencia de espacio	Define las opciones de eficiencia de espacio para las máquinas virtuales que se implementan en el almacén de datos. Seleccione una de las siguientes opciones: ■ **Desduplicación y compresión**: especifique esta opción si desea aplicar tanto la desduplicación como la compresión a los datos. ■ **Solo compresión**: especifique esta opción si desea aplicar solo compresión a los datos. **Nota** Para vSAN Original Storage Architecture, la compresión es una configuración de nivel de clúster. Para vSAN Express Storage Architecture, la opción de solo compresión se aplica en el nivel de objeto. Eso significa que puede usar la compresión para una máquina virtual, pero no para otra del mismo clúster. ■ **Sin eficiencia de espacio**: especifique esta opción si no desea aplicar compresión a los objetos. ■ **Sin preferencia**: especifique esta opción si no desea aplicar explícitamente ninguna regla de eficiencia de espacio. Al seleccionar esta opción, vSAN aplicará todas las reglas de eficiencia de espacio a las máquinas virtuales.
Nivel de almacenamiento	Especifique el nivel de almacenamiento para todas las máquinas virtuales con la directiva de almacenamiento definida. Seleccione una de las siguientes opciones: ■ **Basado íntegramente en tecnología flash**: especifique esta opción si desea que sus máquinas virtuales sean compatibles con entornos basados íntegramente en tecnología flash. ■ **Híbrido**: especifique esta opción si desea que las máquinas virtuales sean compatibles solo con entornos híbridos. ■ **Sin preferencia**: especifique esta opción si no desea aplicar explícitamente ninguna regla de nivel de almacenamiento. Al seleccionar esta opción, vSAN hará que las máquinas virtuales sean compatibles con entornos híbridos y basados íntegramente en flash.

Tabla 7-3. Directiva de almacenamiento: reglas de directiva avanzadas

Funcionalidad	Descripción
Número de fracciones de disco por objeto	El número mínimo de dispositivos de capacidad entre los que se fracciona cada réplica de un objeto de una máquina virtual. Un valor mayor que 1 produce un mejor rendimiento, pero también un mayor uso de los recursos del sistema. El valor predeterminado es 1 y el máximo es 12. No cambie el valor de fraccionamiento predeterminado. En un entorno híbrido, las fracciones de discos se distribuyen entre discos magnéticos. Para una configuración basada en flash, el fraccionamiento se realiza entre los dispositivos flash que conforman la capa de capacidad. Asegúrese de que el entorno de vSAN tenga suficientes dispositivos de capacidad presentes para adecuarse a la solicitud.
Límite de IOPS para objeto	Define el límite de IOPS para un objeto, como VMDK. El valor de IOPS se calcula como el número de operaciones de E/S, utilizando un tamaño ponderado. Si el sistema utiliza el tamaño de base predeterminado de 32 KB, una E/S de 64 KB representa dos operaciones de E/S. Al calcular las IOPS, la lectura y escritura se consideran equivalentes, pero no se consideran la proporción de aciertos de la memoria caché ni la secuencialidad. Si las IOPS de un disco exceden el límite, se aceleran las operaciones de E/S. Si **Límite de IOPS para objeto** se establece en 0, no se aplicarán los límites de IOPS. vSAN permite que el objeto duplique la tasa del límite de E/S por segundo durante el primer segundo de la operación o después de un período de inactividad.
Reserva de espacio de objetos	Porcentaje del tamaño lógico del objeto de disco de máquina virtual (vmdk) que se debe reservar o al que se debe aplicar aprovisionamiento grueso al implementar las máquinas virtuales. Se encuentran disponibles las siguientes opciones: ■ Aprovisionamiento fino (predeterminado) ■ 25 % de reserva ■ 50 % de reserva ■ 75 % de reserva ■ Aprovisionamiento grueso

Tabla 7-3. Directiva de almacenamiento: reglas de directiva avanzadas (continuación)

Funcionalidad	Descripción
Reserva de Flash Read Cache (%)	La capacidad flash reservada como memoria caché de lectura para el objeto de la máquina virtual. Se especifica como un porcentaje del tamaño lógico del objeto del disco de la máquina virtual (vmdk). La capacidad flash reservada no puede ser utilizada por otros objetos. La capacidad flash no reservada se comparte de manera equitativa entre todos los objetos. Utilice esta opción solamente para solucionar problemas de rendimiento específicos. No es necesario establecer una reserva para obtener memoria caché. La configuración de las reservas de memoria caché de lectura podría ocasionar problemas cuando se transfiere el objeto de la máquina virtual, debido a que los ajustes de reserva de la memoria caché siempre se incluyen con el objeto. El atributo de la directiva de almacenamiento de reserva de Flash Read Cache solo es compatible con las configuraciones de almacenamiento híbridas. No utilice este atributo al definir una directiva de almacenamiento de máquina virtual para un clúster basado íntegramente en tecnología flash ni para un clúster de vSAN ESA. El valor predeterminado es 0 %. El valor máximo es 100 %. **Nota** Como opción predeterminada, vSAN asigna memoria caché de lectura de manera dinámica a los objetos de almacenamiento en función de la demanda. Esta característica representa el uso más flexible y más óptimo de los recursos. Como consecuencia, por lo general, no es necesario cambiar el valor predeterminado de 0 para este parámetro. Si desea aumentar el valor en el momento de solucionar un problema de rendimiento, sea cuidadoso. El sobreaprovisionamiento de reservas de memoria caché entre varias máquinas virtuales puede implicar un desperdicio de espacio en el dispositivo flash por reservas excesivas. Estas reservas de memoria caché no se pueden usar para atender las cargas de trabajo para las que se necesita espacio en cierto momento. Este desperdicio de espacio y falta de disponibilidad podrían causar una degradación en el rendimiento.

Tabla 7-3. Directiva de almacenamiento: reglas de directiva avanzadas (continuación)

Funcionalidad	Descripción
Suma de comprobación de objeto	Si la opción se establece en **No**, el objeto calcula la información de suma de comprobación para garantizar la integridad de sus datos. Si esta opción se establece en **Sí**, el objeto no calcula la información de suma de comprobación. vSAN utiliza la suma de comprobación de extremo a extremo para garantizar la integridad de los datos confirmando que cada copia de un archivo sea exactamente igual que el archivo de origen. El sistema comprueba la validez de los datos durante las operaciones de lectura/escritura y, si se detecta un error, vSAN repara los datos o informa del error. Si se detecta una discrepancia en la suma de comprobación, vSAN repara automáticamente los datos sobrescribiendo los datos incorrectos con los datos correctos. Se realiza el cálculo de la suma de comprobación y la corrección de errores como operaciones en segundo plano. La configuración predeterminada para todos los objetos del clúster es **No**, lo que significa que la suma de comprobación está habilitada. **Nota** Para vSAN Express Storage Architecture, la suma de comprobación del objeto siempre está activada y no se puede desactivar.
Forzar aprovisionamiento	Si la opción se establece en **Sí**, el objeto se aprovisiona incluso cuando el almacén de datos no puede satisfacer las directivas **Errores que se toleran**, **Número de fracciones de disco por objeto** y **Reserva de Flash Read Cache** especificadas en la directiva de almacenamiento. Use este parámetro en escenarios de arranque y durante una interrupción cuando el aprovisionamiento estándar ya no sea posible. El valor predeterminado **No** es aceptable para la mayoría de los entornos de producción. vSAN no aprovisiona una máquina virtual cuando no se cumplen los requisitos de la directiva; sin embargo, crea correctamente la directiva de almacenamiento definida por el usuario.

Al trabajar con directivas de almacenamiento de máquinas virtuales, debe comprender la manera en que las funcionalidades de almacenamiento afectan al uso de la capacidad de almacenamiento en el clúster de vSAN. Para obtener más información sobre las consideraciones de diseño y definición de tamaño de las directivas de almacenamiento, consulte "Diseñar un clúster de vSAN y definir su tamaño" en *Planificar e implementar vSAN*.

Cómo vSAN administra los cambios de directivas

vSAN 6.7 Update 3 y las versiones posteriores administran los cambios de directivas para reducir la cantidad de espacio transitorio que se consume en todo el clúster.

La capacidad transitoria se genera cuando vSAN vuelve a configurar objetos para un cambio de directiva.

Cuando se modifica una directiva, el cambio se acepta, pero no se aplica de inmediato. vSAN procesa por lotes las solicitudes de cambios de directivas y las ejecuta de forma asíncrona para mantener una cantidad fija de espacio transitorio.

Los cambios de directivas se rechazan inmediatamente si los motivos no se relacionan con la capacidad, como el cambio de una directiva de RAID-5 a RAID-6 en un clúster de cinco hosts.

Es posible ver el uso de capacidad transitoria en el monitor de capacidad de vSAN. Para comprobar el estado de un cambio de directiva en un objeto, use vSAN Health Service para comprobar el estado del objeto vSAN.

Ver los proveedores de almacenamiento de vSAN

Al habilitar vSAN, automáticamente se configura y se registra un proveedor de almacenamiento para cada host del clúster de vSAN.

Los proveedores de almacenamiento de vSAN son componentes de software integrados que comunican las funcionalidades del almacén de datos a vCenter Server. Una capacidad de almacenamiento generalmente se representa mediante un par clave-valor, en la que la clave es una propiedad específica que ofrece el almacén de datos. El valor es un número o rango que el almacén de datos puede proporcionar para un objeto aprovisionado, como un objeto del espacio de nombres del directorio principal de la máquina virtual o un disco virtual. También puede usar etiquetas para crear funcionalidades de almacenamiento definidas por el usuario y hacer referencia a ellas al definir una directiva de almacenamiento para una máquina virtual. Para obtener más información sobre cómo aplicar y utilizar etiquetas con los almacenes de datos, consulte la documentación de *Almacenamiento de vSphere*.

Los proveedores de almacenamiento de vSAN informan de un conjunto de funcionalidades de almacenamiento subyacentes a vCenter Server. Asimismo, se comunican con la capa de vSAN para informar de los requisitos de almacenamiento de las máquinas virtuales. Para obtener más información sobre proveedores de almacenamiento, consulte el documento *Almacenamiento de vSphere*.

vSAN 6.7 y versiones posteriores registran solo un proveedor de almacenamiento de vSAN para todos los clústeres de vSAN administrados por vCenter Server mediante la siguiente URL:

```
https://<VC fqdn>:<VC https port>/vsan/vasa/version.xml
```

Compruebe que los proveedores de almacenamiento estén registrados.

Procedimiento

1 Desplácese hasta vCenter Server.

2 Haga clic en la pestaña **Configurar** y, a continuación, en **Proveedores de almacenamiento**.

Resultados

El proveedor de almacenamiento para vSAN se muestra en la lista.

Nota No es posible eliminar del registro de forma manual a los proveedores de almacenamiento que utiliza vSAN. Para quitar los proveedores de almacenamiento de vSAN o eliminarlos del registro, quite los hosts correspondientes del clúster de vSAN y luego vuelva a agregarlos. Asegúrese de que haya al menos un proveedor de almacenamiento activo.

¿Cuáles son las directivas de almacenamiento predeterminadas de vSAN?

vSAN requiere que a las máquinas virtuales implementadas en los almacenes de datos de vSAN se les asigne, al menos, una directiva de almacenamiento.

Al aprovisionar una máquina virtual, si no le asigna una directiva de almacenamiento de manera explícita, vSAN le asignará una directiva de almacenamiento predeterminada. Cada directiva predeterminada contiene conjuntos de reglas de vSAN y un conjunto de funcionalidades básicas de almacenamiento que generalmente se usan para ubicar las máquinas virtuales implementadas en los almacenes de datos de vSAN.

Tabla 7-4. Especificaciones de la directiva de almacenamiento predeterminada de vSAN

Especificación	Configuración
Errores que se toleran	1
Número de fracciones de disco por objeto	1
Reserva de Flash Read Cache o capacidad flash utilizada para la memoria caché de lectura	0
Reserva de espacio de objetos	0 **Nota** Cuando la reserva de espacio de objetos se configura en 0, el disco virtual se aprovisiona con formato fino, de forma predeterminada.
Forzar aprovisionamiento	No

Si utiliza un clúster de vSAN Express Storage Architecture, en función del tamaño de su clúster, podrá utilizar una de las directivas de ESA especificadas aquí.

Tabla 7-5. Especificaciones de la directiva de almacenamiento predeterminada de vSAN ESA - RAID-5

Especificación	Configuración
Errores que se toleran	1
Número de fracciones de disco por objeto	1
Reserva de Flash Read Cache o capacidad flash utilizada para la memoria caché de lectura	0
Reserva de espacio de objetos	Aprovisionamiento fino
Forzar aprovisionamiento	No

Nota RAID-5 en vSAN ESA admite tres clústeres de hosts. Si habilita la administración de directivas automática, el clúster deberá tener cuatro hosts para usar RAID-5.

Tabla 7-6. Especificaciones de la directiva de almacenamiento predeterminada de vSAN ESA - RAID-6

Especificación	Configuración
Errores que se toleran	2
Número de fracciones de disco por objeto	1
Reserva de Flash Read Cache o capacidad flash utilizada para la memoria caché de lectura	0
Reserva de espacio de objetos	Aprovisionamiento fino
Forzar aprovisionamiento	No

Nota Para utilizar RAID-6, debe tener al menos seis hosts en el clúster.

Si desea revisar las opciones de configuración de la directiva de almacenamiento predeterminada de máquina virtual, desplácese hasta **Directivas de almacenamiento de máquina virtual** > nombre d la directiva de almacenamiento predeterminada > **Conjunto de reglas 1: vSAN**.

Para obtener mejores resultados, considere la posibilidad de crear y usar sus propias directivas de almacenamiento de máquina virtual, aunque los requisitos de la directiva sean iguales a los definidos en la directiva de almacenamiento predeterminada. En algunos casos, al escalar un clúster, debe modificar la directiva de almacenamiento predeterminada para mantener el cumplimiento de los requisitos del Acuerdo de nivel de servicio para VMware Cloud on AWS.

Cuando se asigna una directiva de almacenamiento definida por el usuario a un almacén de datos, vSAN aplica la configuración de la directiva definida por el usuario al almacén de datos especificado. Solo una directiva de almacenamiento puede ser la directiva predeterminada para el almacén de datos de vSAN.

Características de la directiva de almacenamiento predeterminada de vSAN

Las siguientes características se aplican a las directivas de almacenamiento predeterminadas de almacén de datos de vSAN.

- Una directiva de almacenamiento predeterminada de almacén de datos de vSAN se asignará a todos los objetos de máquina virtual si no se asigna ninguna otra directiva de vSAN al aprovisionar una máquina virtual. El cuadro de texto **Directiva de almacenamiento de máquina virtual** se configura como **Valor predeterminado de almacén de datos** en la página Seleccionar almacenamiento. Para obtener más información sobre el uso de las directivas de almacenamiento, consulte el documento *Almacenamiento de vSphere*.

  Nota Los objetos de intercambio de máquina virtual y de memoria de máquina virtual reciben una directiva de almacenamiento predeterminada de vSAN cuando **Forzar aprovisionamiento** se establece en **Sí**.

- Una directiva predeterminada de vSAN solo se aplica a los almacenes de datos de vSAN. No es posible aplicar una directiva de almacenamiento predeterminada a almacenes de datos no pertenecientes a vSAN (por ejemplo, un almacén de datos de NFS o VMFS).
- Los objetos en un clúster de vSAN Express Storage Architecture con configuración RAID 0 o RAID 1 tendrán 3 fracciones de disco, aunque la directiva predeterminada solo defina una.
- Debido a que la directiva de almacenamiento predeterminada de vSAN es compatible con cualquier almacén de datos de vSAN en vCenter Server, puede mover los objetos de máquinas virtuales aprovisionados con la directiva predeterminada a cualquier almacén de datos de vSAN en vCenter Server.
- Puede clonar la directiva predeterminada y usarla como plantilla para crear una directiva de almacenamiento definida por el usuario.
- Si tiene el privilegio *StorageProfile.View*, podrá editar la directiva predeterminada. Debe tener al menos un clúster habilitado para vSAN que contenga al menos un host. Por lo general, la configuración de la directiva de almacenamiento predeterminada no se modifica.
- No es posible editar el nombre ni la descripción de la directiva predeterminada, ni tampoco la especificación del proveedor de almacenamiento de vSAN. Todos los demás parámetros, incluidas las reglas de la directiva, pueden editarse.
- No puede eliminar la directiva de almacenamiento predeterminada.
- Una directiva de almacenamiento predeterminada se asigna cuando la directiva que asigna durante el aprovisionamiento de máquinas virtuales no incluye reglas específicas para vSAN.

Administración de directivas automáticas

Los clústeres con vSAN Express Storage Architecture pueden usar la administración de directivas automáticas para generar una directiva de almacenamiento predeterminada óptima en función del tipo de clúster (estándar o ampliado) y del número de hosts. vSAN configura las opciones **Tolerancia ante desastres del sitio** y **Errores que se toleran** a una configuración óptima para el clúster.

El nombre de la directiva generada automáticamente se basa en el nombre del clúster de la siguiente forma: *NombreClúster - Directiva de almacén de datos predeterminada*

Si habilita la opción Directiva automática, vSAN asignará una nueva directiva óptima al almacén de datos de vSAN, y esa directiva se convertirá en la directiva predeterminada del almacén de datos para el clúster.

Para habilitar la administración de directivas automáticas, utilice el control deslizante situado en **vSAN > Servicios > Almacenamiento > Editar**.

Cambiar la directiva de almacenamiento predeterminada de los almacenes de datos de vSAN

Es posible cambiar la directiva de almacenamiento predeterminada para un almacén de datos de vSAN seleccionado.

Requisitos previos

Compruebe que la directiva de almacenamiento de máquina virtual que desea asignar como la directiva predeterminada para el almacén de datos de vSAN cumpla con los requisitos de las máquinas virtuales del clúster de vSAN.

Procedimiento

1 Vaya hasta el almacén de datos de vSAN.

2 Haga clic en **Configurar**.

3 En **General**, haga clic en el botón **Editar** de la directiva de almacenamiento predeterminada y seleccione la directiva de almacenamiento que desea asignar como la predeterminada para el almacén de datos de vSAN.

   Nota También puede editar la directiva de almacenamiento de inicio de disco virtual mejorada. Haga clic en **Editar** y seleccione la directiva de almacenamiento de inicio que desea asignar como directiva de almacenamiento para el objeto de inicio.

   Puede elegir entre una lista de directivas de almacenamiento compatibles con el almacén de datos de vSAN, como la directiva de almacenamiento predeterminada de vSAN y las directivas de almacenamiento definidas por el usuario que contienen conjuntos de reglas de vSAN definidos.

4 Seleccione una directiva y haga clic en **Aceptar**.

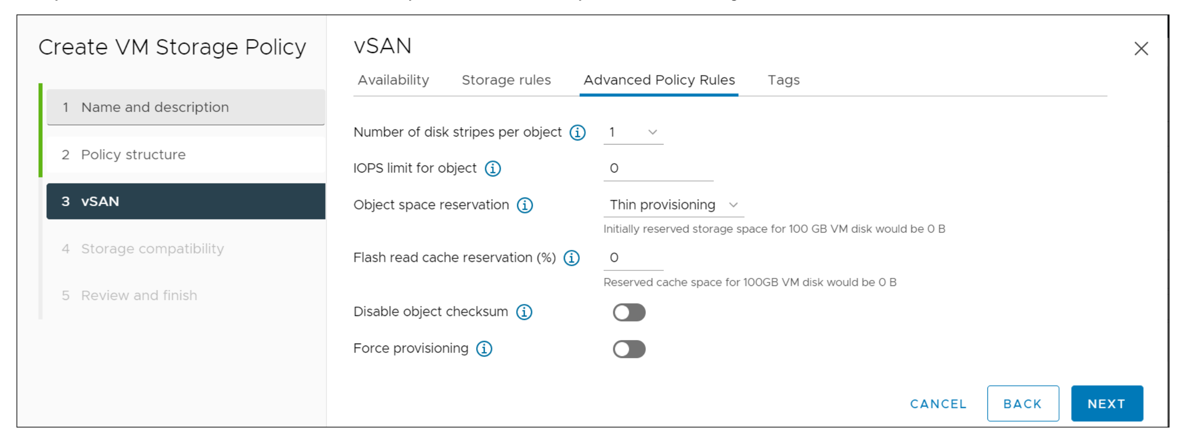
   La directiva de almacenamiento se aplica como la directiva predeterminada al aprovisionar las nuevas máquinas virtuales sin especificar una directiva de almacenamiento de manera explícita para un almacén de datos.

Pasos siguientes

Puede definir una nueva directiva de almacenamiento para máquinas virtuales. Consulte Definir una directiva de almacenamiento de vSAN mediante vSphere Client.

Definir una directiva de almacenamiento de vSAN mediante vSphere Client

Es posible crear una directiva de almacenamiento en la que se definan los requisitos de almacenamiento para una máquina virtual y sus discos virtuales.



En esta directiva, debe hacer referencia a las capacidades de almacenamiento que admite el almacén de datos de vSAN.

Requisitos previos

- Compruebe que el proveedor de almacenamiento de vSAN esté disponible. Consulte Ver los proveedores de almacenamiento de vSAN.
- Privilegios requeridos: **Almacenamiento basado en perfiles.Vista de almacenamiento basado en perfiles** y **Almacenamiento basado en perfiles.Actualización de almacenamiento basado en perfiles**

Nota Los clústeres con vSAN Express Storage Architecture pueden utilizar la administración de directivas automáticas. Para obtener más información, consulte ¿Cuáles son las directivas de almacenamiento predeterminadas de vSAN?.

Procedimiento

1. Desplácese hasta **Directivas y perfiles** y haga clic en **Directivas de almacenamiento de máquina virtual**.
2. Haga clic en **Crear**.
3. En la página de nombre y descripción, seleccione un vCenter Server.
4. Escriba un nombre y una descripción para la directiva de almacenamiento y haga clic en **Siguiente**.
5. En la página Estructura de directiva, seleccione Habilitar reglas para el almacenamiento "vSAN" y haga clic en **Siguiente**.

6 En la página vSAN, defina el conjunto de reglas de la directiva y haga clic en **Siguiente**.

a En la pestaña Disponibilidad, defina las opciones **Tolerancia ante desastres de sitio** y **Errores que se toleran**.

Las opciones de disponibilidad definen las reglas de errores que se toleran, la ubicación de los datos y el método de tolerancia a errores.

- En **Tolerancia ante desastres de sitio**, se define el tipo de tolerancia ante errores en el sitio que se utilizará para objetos de máquina virtual.
- En **Errores que se toleran**, se definen el número de errores de host y de dispositivo que un objeto de máquina virtual puede tolerar y el método de replicación de datos.

Por ejemplo, si elige **Creación de reflejo de sitio doble** y **2 errores - RAID-6 (codificación de borrado)**, vSAN configura las reglas de directivas siguientes:

- Errores que se toleran: 1
- Nivel secundario de errores que se toleran: 2
- Localidad de datos: Ninguna
- Método de tolerancia a errores: RAID-5/6 (codificación de borrado) - Capacidad

b En la pestaña Reglas de almacenamiento , defina las reglas de cifrado, eficiencia de espacio y nivel de almacenamiento que se pueden utilizar junto con la malla de HCI para distinguir los almacenes de datos remotos.

- **Servicios de cifrado**: define las reglas de cifrado para las máquinas virtuales que implemente con esta directiva. Puede elegir una de las siguientes opciones:
  - **Cifrado de datos en reposo**: el cifrado está habilitado en las máquinas virtuales.
  - **Sin cifrado**: el cifrado no está habilitado en las máquinas virtuales.
  - **Sin preferencia**: hace que las máquinas virtuales sean compatibles con las opciones Cifrado de datos en reposo y Sin cifrado.
- **Eficiencia de espacio**: define las reglas de ahorro de espacio para las máquinas virtuales que implemente con esta directiva. Puede elegir una de las siguientes opciones:
  - **Desduplicación y compresión**: habilita la desduplicación y la compresión en las máquinas virtuales. La desduplicación y compresión están disponibles solo en grupos de discos basados íntegramente en tecnología flash. Para obtener más información, consulte Consideraciones de diseño de desduplicación y compresión en un clúster de vSAN.
  - **Solo compresión**: habilita solo la compresión en las máquinas virtuales. La compresión está disponible solo en grupos de discos basados íntegramente en tecnología flash. Para obtener más información, consulte Consideraciones de diseño de desduplicación y compresión en un clúster de vSAN.

        - **Sin eficiencia de espacio**: las funciones de eficiencia de espacio no están habilitadas en las máquinas virtuales. Para elegir esta opción, se requieren almacenes de datos sin opciones de eficiencia de espacio activas.
        - **Sin preferencia**: hace que las máquinas virtuales sean compatibles con todas las opciones.
    - **Nivel de almacenamiento**: especifica el nivel de almacenamiento para las máquinas virtuales que implemente con esta directiva. Puede elegir una de las siguientes opciones. Si elige **Sin preferencia**, las máquinas virtuales serán compatibles con los entornos híbridos y basados íntegramente en tecnología flash.
        - **Basado íntegramente en tecnología flash**
        - **Híbrido**
        - **Sin preferencia**

   c En la pestaña Reglas de directivas avanzadas, defina las reglas de directivas avanzadas (por ejemplo, el número de fracciones de disco por objeto y los límites de IOPS).

   d En la pestaña Etiquetas, haga clic en **Agregar regla de etiqueta** y defina las opciones de la regla de etiqueta.

   Asegúrese de proporcionar valores que se ubiquen dentro del rango de valores anunciado por las funcionalidades de almacenamiento del almacén de datos de vSAN.

7 En la página Compatibilidad de almacenamiento, consulte la lista de almacenes de datos en las pestañas **COMPATIBLE** e **INCOMPATIBLE** y haga clic en **Siguiente**.

   Para cumplir las condiciones, un almacén de datos no necesita satisfacer todos los conjuntos de reglas incluidos en la directiva. El almacén de datos debe satisfacer al menos uno de los conjuntos de reglas y todas las reglas de dicho conjunto. Verifique que el almacén de datos de vSAN cumpla con los requisitos establecidos en la directiva de almacenamiento y que figure en la lista de almacenes de datos compatibles.

8 En la página Revisar y finalizar, revise la configuración de la directiva y haga clic en **Finalizar**.

Resultados

La nueva directiva se agrega a la lista.

Pasos siguientes

Asigne esta directiva a una máquina virtual y sus discos virtuales. vSAN coloca los objetos de máquina virtual según los requisitos especificados en la directiva. Para obtener información sobre cómo aplicar directivas de almacenamiento a objetos de máquinas virtuales, consulte el documento *Almacenamiento de vSphere*.

Expandir y administrar un clúster de vSAN

8

Después de configurar el clúster de vSAN, puede agregar hosts y dispositivos de capacidad, quitar hosts y dispositivos, y administrar escenarios de errores.

Lea los siguientes temas a continuación:

- Expandir un clúster de vSAN
- Compartir almacenes de datos remotos de vSAN
- Trabajar con miembros del clúster de vSAN en modo de mantenimiento
- Administrar dominios de errores en clústeres de vSAN
- Usar vSAN Data Protection
- Usar el servicio del destino iSCSI de vSAN
- Servicio de archivos de vSAN
- Migrar un clúster híbrido de vSAN a un clúster basado íntegramente en tecnología flash
- Apagar y reiniciar el clúster de vSAN

Expandir un clúster de vSAN

Puede expandir un clúster existente de vSAN agregando hosts o dispositivos a los hosts existentes sin interrumpir las operaciones en curso.

Use uno de los siguientes métodos para expandir el clúster de vSAN.

- Agregue al clúster hosts ESXi nuevos que estén configurados mediante dispositivos compatibles de memoria caché y de capacidad. Consulte Agregar un host al clúster de vSAN.
- Transfiera hosts existentes de ESXi al clúster de vSAN y configúrelos usando el perfil de host. Consulte Configurar hosts en el clúster de vSAN mediante un perfil de host.
- Agregue nuevos dispositivos de capacidad a hosts ESXi que sean miembros del clúster. Consulte Agregar dispositivos al grupo de discos en un clúster de vSAN.

Expandir la capacidad y el rendimiento de un clúster de vSAN

Si el clúster de vSAN se queda sin capacidad de almacenamiento o si detecta una reducción del rendimiento, puede expandir la capacidad y el rendimiento del clúster.

- (Solo para vSAN Original Storage Architecture) Expanda la capacidad de almacenamiento del clúster agregando dispositivos de almacenamiento a los grupos de discos existentes o agregando grupos de discos. Los grupos de discos nuevos requieren dispositivos flash para la memoria caché. Para obtener información sobre cómo agregar dispositivos a grupos de discos, consulte Agregar dispositivos al grupo de discos en un clúster de vSAN. Agregar dispositivos de capacidad sin aumentar la memoria caché puede reducir la proporción entre caché y capacidad a un nivel no compatible. Para obtener más información, consulte *Planificación e implementación de vSAN*.

  Para mejorar el rendimiento del clúster, agregue al menos un dispositivo de memoria caché (flash) y un dispositivo de capacidad (flash o disco magnético) a un controlador de E/S de almacenamiento existente o a un host nuevo. También puede agregar uno o varios hosts con grupos de discos para producir el mismo impacto en el rendimiento después de que vSAN complete un reequilibrio automático en el clúster de vSAN.

- (Solo para vSAN Express Storage Architecture) Expanda la capacidad de almacenamiento del clúster agregando dispositivos flash a los grupos de almacenamiento de los hosts existentes o agregando uno o varios hosts nuevos con dispositivos flash.

Si bien los hosts solo con recursos informáticos pueden existir en un clúster de vSAN y pueden consumir capacidad de otros hosts del clúster, agregue hosts con una configuración uniforme para lograr un funcionamiento eficiente. A pesar de que es mejor utilizar dispositivos idénticos o similares en los grupos de discos o grupos de almacenamiento, cualquier dispositivo incluido en la HCL de vSAN es compatible. Intente distribuir la capacidad de manera uniforme entre los hosts. Para obtener información sobre cómo agregar dispositivos a grupos de discos o grupos de almacenamiento, consulte Crear un grupo de discos o un grupo de almacenamiento en un clúster de vSAN.

Después de expandir la capacidad del clúster, habilite un reequilibrio automático para distribuir equitativamente los recursos en el clúster. Para obtener más información, consulte *Supervisión y solución de problemas de vSAN*.

Utilizar el inicio rápido para agregar hosts a un clúster de vSAN

Si configuró el clúster de vSAN a través del inicio rápido, puede usar el flujo de trabajo de inicio rápido para agregar hosts y dispositivos de almacenamiento al clúster.

Cuando agregue nuevos hosts al clúster de vSAN, puede utilizar el asistente de configuración de clúster para completar la configuración del host. Para obtener más información acerca del inicio rápido, consulte "Usar el inicio rápido para configurar y expandir un clúster de vSAN" en *Planificar e implementar vSAN*.

Nota Si ejecuta vCenter Server en un host, el host no puede colocarse en modo de mantenimiento cuando se agrega a un clúster mediante el flujo de trabajo de inicio rápido. El mismo host también puede estar ejecutando una instancia de Platform Services Controller. Todas las demás máquinas virtuales en el host deben estar apagadas.

Requisitos previos

- El flujo de trabajo de inicio rápido debe estar disponible para el clúster de vSAN.
- Ninguna configuración de red realizada a través del flujo de trabajo de inicio rápido se modificó desde fuera del flujo de trabajo de inicio rápido.
- No se modificó la configuración de redes configurada al crear el clúster con el inicio rápido.

Procedimiento

1. Desplácese hasta el clúster en vSphere Client.
2. Haga clic en la pestaña Configurar y seleccione **Configuración > Inicio rápido**.
3. En la tarjeta Agregar hosts, haga clic en **Iniciar** para abrir el asistente Agregar hosts.
    a. En la página Agregar hosts, introduzca la información de nuevos hosts, o bien haga clic en Hosts existentes y seleccione los hosts que aparecen en el inventario.
    b. En la página Resumen del host, compruebe la configuración del host.
    c. En la página Listo para finalizar, haga clic en **Finalizar**.
4. En la tarjeta Configuración del clúster, haga clic en **Iniciar** para abrir el asistente de configuración del clúster.
    a. En la página Configurar los Distributed Switch, introduzca la configuración de redes de los hosts nuevos.
    b. (opcional) En la página Reclamar discos, seleccione los discos en cada host nuevo.
    c. (opcional) En la página Crear dominios de errores, mueva los nuevos hosts a sus correspondientes dominios de errores.

        Para obtener más información sobre los dominios de errores, consulte Administrar dominios de errores en clústeres de vSAN.
    d. En la página Listo para completar, compruebe la configuración del clúster y haga clic en **Finalizar**.

Agregar un host al clúster de vSAN

Puede agregar hosts ESXi a un clúster de vSAN en ejecución sin interrumpir las operaciones en curso.

Los recursos del host nuevo se asociarán al clúster.

Requisitos previos

- Compruebe que los recursos, incluidos los controladores, el firmware y los controladores de E/S de almacenamiento, aparezcan en el sitio web de la Guía de compatibilidad de VMware en http://www.vmware.com/resources/compatibility/search.php.
- VMware recomienda crear hosts configurados de manera uniforme en el clúster de vSAN a fin de que pueda obtener una distribución homogénea de los componentes y los objetos en los dispositivos del clúster. Sin embargo, pueden haber situaciones en las que el clúster no esté equilibrado de manera homogénea, especialmente durante el mantenimiento o si se sobreasigna la capacidad del almacén de datos de vSAN con implementaciones excesivas de máquinas virtuales.

Procedimiento

1 Desplácese hasta el clúster de vSAN.

2 Haga clic con el botón derecho en el clúster y seleccione **Agregar hosts**. Se mostrará el asistente Agregar hosts.

Opción	Descripción
Nuevos hosts	a Introduzca el nombre de host o la dirección IP. b Introduzca el nombre de usuario y la contraseña asociados con el host.
Hosts existentes	a Seleccione los hosts que agregó previamente a vCenter Server.

3 Haga clic en **Siguiente**.

4 Consulte la información de resumen y haga clic en **Siguiente**.

5 Revise la configuración y haga clic en **Finalizar**.

El host se agrega al clúster.

Pasos siguientes

Verifique que la comprobación de estado del equilibrio de disco de vSAN sea de color verde.

Para obtener más información sobre la configuración de clústeres de vSAN y la solución de problemas, consulte "Problemas de configuración del clúster de vSAN" en *Supervisar vSAN y solucionar sus problemas*.

Configurar hosts en el clúster de vSAN mediante un perfil de host

Cuando se tienen varios hosts en el clúster de vSAN, es posible utilizar el perfil de un host de vSAN existente para configurar los hosts del clúster de vSAN.

El perfil de host incluye información sobre la configuración de almacenamiento, la configuración de red y otras características del host. Si piensa crear un clúster con muchos hosts, por ejemplo, 8, 16, 32 o 64 hosts, utilice la función de perfil de host. Los perfiles de host le permiten agregar más de un host a la vez al clúster de vSAN.

Requisitos previos

- Compruebe que el host esté en modo de mantenimiento.
- Compruebe que los componentes de hardware, los controladores, el firmware y los controladores de E/S de almacenamiento se enumeren en la Guía de compatibilidad de VMware en la siguiente URL: http://www.vmware.com/resources/compatibility/search.php.

Procedimiento

1 Cree un perfil de host.

   a Desplácese hasta la vista de Host Profiles.

   b Haga clic en el icono **Extraer perfil de un host** (✚).

   c Seleccione el host que desea utilizar como host de referencia y haga clic en **Next** (Siguiente).

   El host seleccionado debe ser un host activo.

   d Escriba un nombre y una descripción para nuevo perfil y haga clic en **Next** (Siguiente).

   e Revise la información de resumen del nuevo perfil de host y haga clic en **Finish** (Finalizar).

   El nuevo perfil aparece en la lista Host Profile (Perfil del host).

2 Asocie el host al perfil de host deseado.

   a Desde la lista Perfil en la vista de Host Profiles, seleccione el perfil de host que se debe aplicar al host de vSAN.

   b Haga clic en el icono **Asociar o desasociar hosts y clústeres para un perfil de host** ( ).

   c Seleccione el host desde la lista expandida, haga clic en **Attach** (Asociar) y, a continuación, haga clic en el host que desea asociar con el perfil.

   El host se agrega a la lista Attached Entities (Entidades asociadas).

   d Haga clic en **Siguiente**.

   e Haga clic en **Finish** (Finalizar) para completar la operación de asociación del host con el perfil.

3 Separe del perfil de host el host de vSAN al que se hace referencia.

Cuando se asocia un perfil de host a un clúster, los hosts de ese clúster también se asocian al perfil de host. Sin embargo, cuando el perfil de host se separa del clúster, la asociación entre el host o los hosts incluidos en el clúster y el perfil de host permanece intacta.

a Desde la lista Profile (Perfil) en la vista Host Profiles, seleccione el perfil de host que desea separar de un host o un clúster.

b Haga clic en el icono **Asociar o desasociar hosts y clústeres para un perfil de host** ( ).

c Seleccione el host o el clúster desde la lista expandida y haga clic en **Detach** (Separar).

d Haga clic en **Detach All** (Separar todos) para separar todos los hosts y los clústeres del perfil.

e Haga clic en **Siguiente**.

f Haga clic en **Finish** (Finalizar) para completar la operación de desasociación del host del perfil del host.

4 Compruebe que el host de vSAN cumpla con los requisitos del perfil de host asociado y determine si hay parámetros de configuración diferentes a los especificados en el perfil de host.

a Desplácese hasta un perfil de host.

En la pestaña **Objects** (Objetos), se enumeran todos los perfiles de host, la cantidad de hosts asociados con el perfil de host y los resultados resumidos de la última comprobación de cumplimiento.

b Haga clic en el icono **Comprobar cumplimiento de perfil de host** ( ).

Para ver detalles específicos sobre qué parámetros tienen diferencias entre el host con incumplimiento y el perfil de host, haga clic en la pestaña **Monitor** (Supervisar) y seleccione la vista Compliance (Cumplimiento). Expanda la jerarquía de objetos y seleccione el host no compatible. Los parámetros con diferencias se muestran en la ventana Compliance (Cumplimiento), debajo de la jerarquía.

Si se produce un error de cumplimiento, use la acción Remediate (Corregir) para aplicar la configuración del perfil de host al host. Esta acción cambia todos los parámetros administrados por el perfil de host por los valores contenidos en el perfil de host asociado al host.

c Para ver detalles específicos sobre qué parámetros tienen diferencias entre el host con incumplimiento y el perfil de host, haga clic en la pestaña **Monitor** (Supervisar) y seleccione la vista Compliance (Cumplimiento).

d Expanda la jerarquía de objetos y seleccione el host con error.

Los parámetros con diferencias se muestran en la ventana Compliance (Cumplimiento), debajo de la jerarquía.

5 Corrija el host para solucionar los errores de cumplimiento.

  a Seleccione la pestaña **Monitor** (Supervisar) y haga clic en **Compliance** (Cumplimiento).

  b Haga clic con el botón derecho en los hosts y seleccione **All vCenter Actions (Todas las acciones de vCenter) > Host Profiles (Perfiles de host) > Remediate (Corregir)**.

    Puede personalizar el host para actualizar o cambiar los parámetros de entrada del usuario de las directivas de Host Profiles.

  c Haga clic en **Siguiente**.

  d Revise las tareas necesarias para corregir el perfil de host y haga clic en **Finish** (Finalizar).

  El host forma parte del clúster de vSAN y sus recursos están accesibles para el clúster de vSAN. El host también puede acceder a todas las directivas de E/S de almacenamiento de vSAN existentes en el clúster de vSAN.

Compartir almacenes de datos remotos de vSAN

El uso compartido de almacenes de datos remotos permite que los clústeres de vSAN compartan sus almacenes de datos con otros clústeres.

Puede aprovisionar máquinas virtuales que se ejecuten en su clúster local para usar espacio de almacenamiento en un almacén de datos remoto. Al aprovisionar una nueva máquina virtual, puede seleccionar un almacén de datos remoto que esté montado en el clúster de cliente. Asigne una directiva de almacenamiento compatible configurada para el almacén de datos.

Montar un almacén de datos remoto es una configuración que se aplica a todo el clúster. Cuando monte un almacén de datos remoto en un clúster de vSAN, estará disponible en todos los hosts del clúster.

Cuando cree un clúster de vSAN o configure un clúster de vSphere para vSAN, puede seleccionar el tipo de configuración de HCI.

- **vSAN HCI** proporciona recursos informáticos y de almacenamiento. Puede compartir su almacén de datos entre centros de datos y vCenter, y montar almacenes de datos de otros clústeres de vSAN HCI.
- El **clúster de proceso de vSAN** es un clúster de vSphere que solo proporciona recursos informáticos. Puede montar almacenes de datos servidos por clústeres de vSAN Max.
- **vSAN Max** (solo vSAN ESA) proporciona recursos de almacenamiento, pero no recursos informáticos. Su almacén de datos se puede montar mediante clústeres de vSAN HCI o clústeres de vSphere remotos en varios centros de datos y vCenter.

El uso compartido de almacenes de datos de vSAN tiene las siguientes consideraciones de diseño:

- Los clústeres de vSAN Original Storage Architecture que ejecutan la versión 8.0 Update 1 o una posterior pueden compartir almacenes de datos entre clústeres en el mismo centro de datos o entre clústeres administrados por instancias remotas de vCenter, siempre y cuando se encuentren en la misma red. Los clústeres de vSAN Express Storage Architecture que ejecutan la versión 8.0 Update 2 o posteriores tienen esta función.
- Un clúster de vSAN HCI o vSAN Max puede servir su almacén de datos local a un máximo de 10 clústeres de clientes.
- Un clúster de clientes puede montar hasta 5 almacenes de datos remotos de uno o varios clústeres de servidores de vSAN.
- Un solo almacén de datos puede montarse hasta en 128 hosts de vSAN, incluidos hosts en el clúster de servidores de vSAN local.
- Todos los objetos que conforman una máquina virtual deben residir en el mismo almacén de datos.
- Para que vSphere HA funcione con el uso compartido de almacenes de datos de vSAN, configure la siguiente respuesta ante fallos para el almacén de datos con APD: Apagar y reiniciar las máquinas virtuales.
- No se admiten hosts cliente que no formen parte de un clúster. Puede configurar un clúster de un único host solo de proceso, pero vSphere HA no funcionará a menos que agregue un segundo host al clúster.
- No se admite el cifrado de datos en tránsito.

Las siguientes configuraciones no son compatibles con el uso compartido de almacenes de datos de vSAN:

- Aprovisionamiento remoto de volúmenes iSCSI o volúmenes persistentes de CNS. Se pueden aprovisionar en el almacén de datos local de vSAN, pero no en ningún almacén de datos remoto de vSAN.
- Clústeres o redes con espaciado aéreo que usan varios puertos de VMkernel de vSAN.

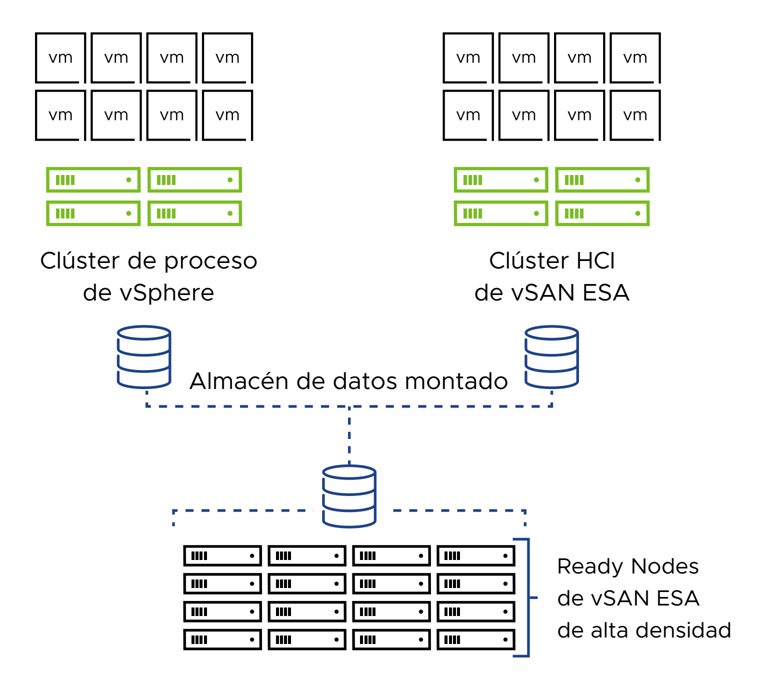
Almacenamiento desagregado con vSAN Max

vSAN Max es una solución de almacenamiento totalmente distribuida, escalable y compartida para clústeres de vSphere y clústeres de vSAN. Los recursos de almacenamiento se separan de los recursos informáticos, lo que permite escalar el almacenamiento y los recursos informáticos de forma independiente.

vSAN Max utiliza vSAN Express Storage Architecture y vSAN Ready Nodes de alta densidad para aumentar la capacidad y el rendimiento.

Nota vSAN Max se puede implementar adquiriendo VMware Cloud Foundation o la oferta del complemento avanzado para VMware vSphere Foundation. La concesión de licencias para vSAN Max se basa en una métrica por TiB, que corresponde a la cantidad total de capacidad de almacenamiento sin procesar necesaria para los entornos.

Un clúster de vSAN Max actúa como un clúster de servidores que solo proporciona almacenamiento. Puede montar su almacén de datos en clústeres de vSphere configurados como clústeres de proceso de vSAN o clústeres de clientes de vSAN HCI.



Los clústeres de vSAN Max tienen las siguientes consideraciones de diseño:

- Solo se admite en vSAN Express Storage Architecture en vSAN Ready Nodes certificados para vSAN Max.
- No es compatible con vSAN Original Storage Architecture.
- Actúa solo como un servidor de almacenamiento, no como un cliente. No ejecute máquinas virtuales de carga de trabajo en hosts de vSAN Max.
- Requiere al menos seis hosts y 150 TiB por host. Para optimizar el rendimiento, utilice una configuración uniforme de dispositivos de almacenamiento en todos los hosts.
- Requiere conexiones de red de 100 Gbps entre los hosts del clúster de vSAN Max y conexiones de 10Gbps desde los clientes de proceso al clúster de vSAN Max. Para obtener el mejor rendimiento, habilite la compatibilidad con tramas gigantes (MTU = 9000) y asegúrese de tener suficientes recursos en el tronco de la red.

- Habilite **Administración de directivas automáticas** (Configurar > vSAN > Servicios > Almacenamiento > Editar) para garantizar niveles óptimos de resistencia y eficiencia de espacio.
- Habilite **Reequilibrio automático** (Configurar > vSAN > Servicios > Opciones avanzadas > Editar) para garantizar un sistema de almacenamiento distribuido y equilibrado de manera uniforme.

Nota Puede configurar vSAN Max solo durante la creación del clúster. No se puede convertir un clúster de vSAN existente a vSAN Max ni vSAN Max en un clúster de vSAN HCI. Debe desactivar vSAN en el clúster y volver a configurar el clúster.

Clúster de proceso de vSAN

Un clúster de proceso de vSAN es un clúster de vSphere con un elemento de vSAN pequeño que le permite montar un almacén de datos de vSAN Max. Los hosts de un clúster de proceso no tiene almacenamiento local. Puede supervisar la capacidad, el estado y el rendimiento del almacén de datos remoto.

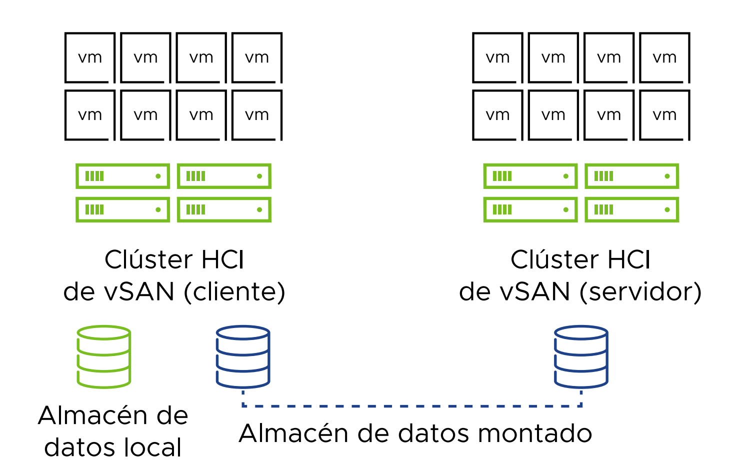
Los clústeres de proceso de vSAN tienen las siguientes consideraciones de diseño:

- Debe haber redes de vSAN configuradas en los hosts del clúster de proceso.
- No puede haber dispositivos de almacenamiento presentes en los hosts de un clúster de proceso.
- No se puede configurar ninguna función de administración de datos en el clúster de proceso.

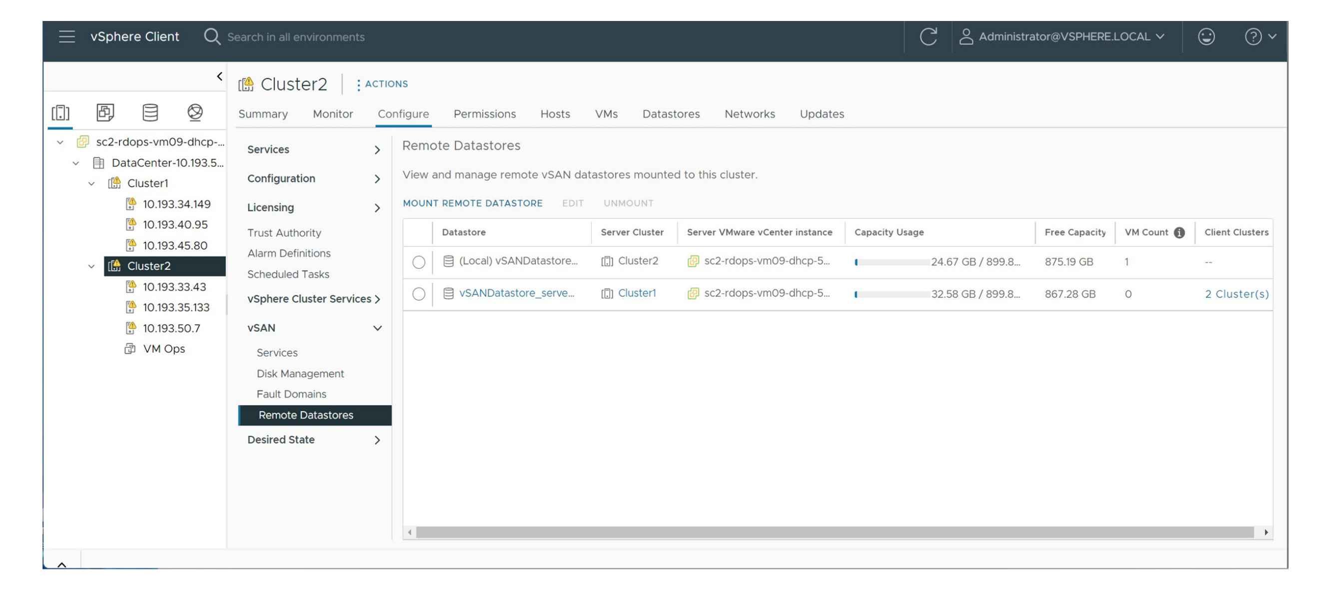
Uso compartido de capacidad entre clústeres

Los clústeres de vSAN HCI pueden compartir sus almacenes de datos con otros clústeres de vSAN HCI. Un clúster de vSAN HCI puede actuar como servidor para proporcionar almacenamiento de datos o como un cliente que consume almacenamiento.

vSAN Original Storage Architecture y vSAN Express Storage Architecture no son compatibles y no pueden compartir almacenes de datos entre sí. Un clúster de clientes no puede montar almacenes de datos de diferentes arquitecturas de vSAN. Si un clúster montó un almacén de datos que utiliza vSAN Original Storage Architecture, no podrá montar un almacén de datos que use vSAN Express Storage Architecture.



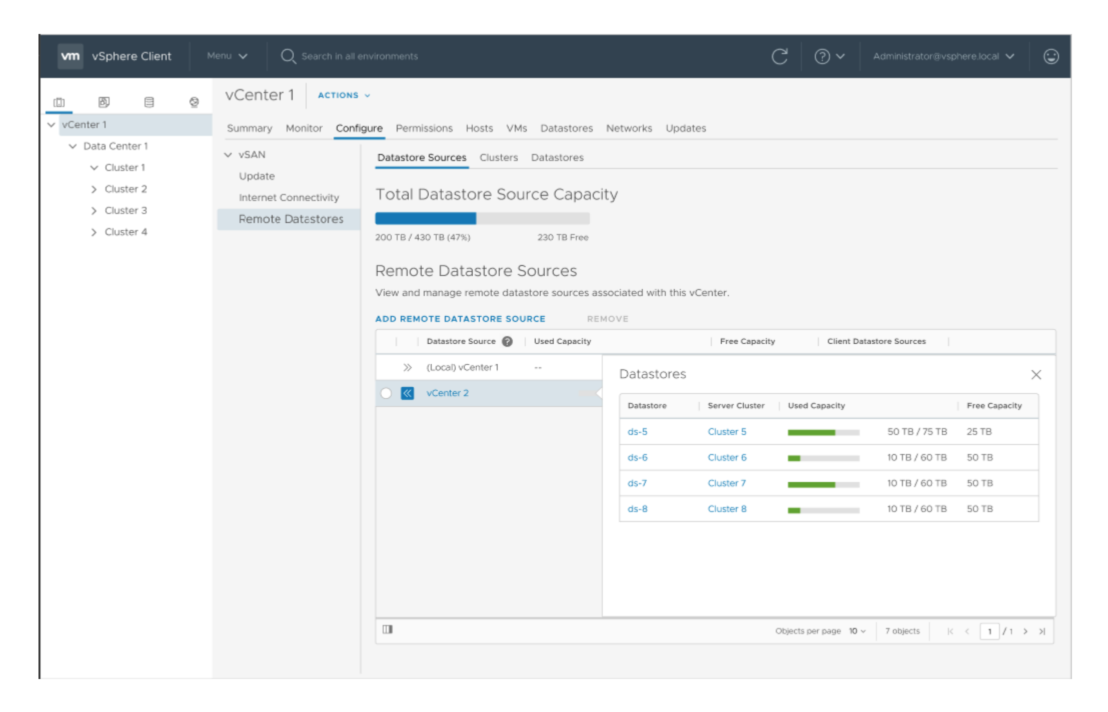
Use la vista Almacenes de datos remotos para supervisar y administrar almacenes de datos remotos montados en el clúster de vSAN local. Cada clúster de clientes de vSAN puede montar almacenes de datos remotos desde clústeres de servidores de vSAN. Cada clúster de vSAN compatible también puede actuar como un servidor y permitir que otros clústeres de vSAN monten su almacén de datos local.



Las vistas de supervisión de la capacidad, el rendimiento, el estado y la ubicación de los objetos virtuales muestran el estado de los almacenes de datos y los objetos remotos.

Usar instancias remotas de vCenter como orígenes de almacenes de datos

Los clústeres de vSAN HCI y vSAN Max pueden compartir almacenes de datos remotos entre instancias de vCenter. Puede agregar una instancia remota de vCenter como origen de almacén de datos para los clústeres en la instancia local de vCenter. Los clústeres de clientes en la instancia local de vCenter pueden montar almacenes de datos que residen en la instancia remota de vCenter.



Utilice la página Almacenes de datos remotos de vCenter para administrar orígenes de almacenes de datos remotos (**Configurar > vSAN > Almacenes de datos remotos**). Haga clic en las pestañas para acceder a información sobre los almacenes de datos compartidos entre las instancias de vCenter, agregar instancias de vCenter como orígenes de almacenes de datos y montar almacenes de datos en clústeres locales.

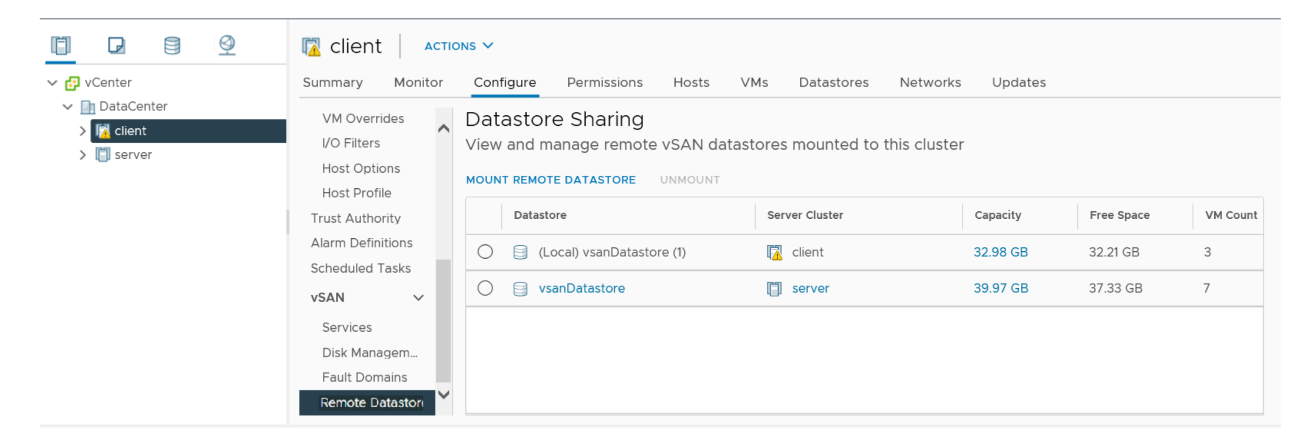
Orígenes de almacén de datos	Ver y administrar orígenes de almacenes de datos que residen en instancias remotas de vCenter. Puede agregar o quitar orígenes de almacenes de datos remotos para la instancia local de vCenter.
Clústeres	Ver y administrar clústeres que residen en la instancia de vCenter local. Puede montar o desmontar almacenes de datos de instancias remotas de vCenter en el clúster seleccionado.
Almacenes de datos	Vea todos los almacenes de datos disponibles en esta instancia de vCenter.

El uso compartido de almacenes de datos de vCenter a vCenter tiene las siguientes consideraciones de diseño:

- Cada instancia de vCenter puede servir a un máximo de 10 instancias de vCenter del cliente.
- Cada instancia de vCenter de cliente puede agregar hasta 5 orígenes de almacenes de datos remotos de vCenter.
- Cuando una máquina virtual en un clúster de clientes administrado por un vCenter utiliza almacenamiento de un servidor administrado por otro vCenter, la directiva de almacenamiento en el vCenter del cliente tendrá prioridad.

Ver almacenes de datos remotos de vSAN

Utilice la página Almacenes de datos remotos para ver los almacenes de datos remotos montados en el clúster de vSAN local y los clústeres de clientes que comparten el almacén de datos local.



Procedimiento

1 Desplácese hasta el clúster de vSAN local.

2 Haga clic en la pestaña Configurar.

3 En vSAN, haga clic en **Almacenes de datos remotos**.

Resultados

Esta vista muestra información sobre cada almacén de datos montado en el clúster local.

- Clúster de servidores que aloja el almacén de datos
- Instancia de vCenter del clúster de servidores (si corresponde)
- Uso de capacidad del almacén de datos
- Capacidad libre disponible
- Número de máquinas virtuales que utilizan el almacén de datos (número de máquinas virtuales que utilizan los recursos informáticos del clúster local, pero los recursos de almacenamiento del clúster de servidores).
- Clústeres de clientes que han montado el almacén de datos

Pasos siguientes

Puede montar o desmontar almacenes de datos remotos desde esta página.

Montar almacén de datos remoto de vSAN

Puede montar uno o varios almacenes de datos de otros clústeres de vSAN.

Procedimiento

1 Desplácese hasta el clúster de vSAN local.

2 Haga clic en la pestaña Configurar.

3 En vSAN, haga clic en **Almacenes de datos remotos**.

4 Haga clic en **Montar almacén de datos remoto** para abrir el asistente.

5 (Opcional) Seleccione una instancia remota de vCenter como origen del almacén de datos.

6 Seleccione un almacén de datos.

7 (Opcional) Si el clúster de servidores es un clúster ampliado de vSAN, configure la combinación de sitios para elegir la ruta de datos óptima entre los clientes y los servidores de vSAN HCI.

   Un clúster ampliado de vSAN puede tener una red asimétrica, donde los vínculos dentro de cada sitio tienen un mayor ancho de banda y una menor latencia que los vínculos entre sitios. Una red simétrica tiene vínculos similares dentro de cada sitio y entre sitios.

   a En la página Topología de red, seleccione **Simétrica** o **Asimétrica**. Si selecciona Asimétrica, se abrirá la página Combinación de sitios.

   b Seleccione un sitio en el clúster de servidores para asociarlo con el sitio del cliente adecuado. Seleccione el sitio del servidor que esté físicamente más cerca o adyacente a cada sitio del cliente.

8 Compruebe la compatibilidad del almacén de datos y haga clic en **Finalizar**.

Resultados

El almacén de datos remoto se montará en el clúster de vSAN local.

Pasos siguientes

Al aprovisionar una máquina virtual, puede seleccionar el almacén de datos remoto como recurso de almacenamiento. Asigne una directiva de almacenamiento que sea compatible con el almacén de datos remoto.

Desmontar almacén de datos remoto de vSAN

Puede desmontar un almacén de datos remoto desde un clúster de vSAN.

Si ninguna máquina virtual del clúster local utiliza el almacén de datos de vSAN remoto, puede desmontar el almacén de datos del clúster de vSAN local.

Procedimiento

1 Desplácese hasta el clúster de vSAN local.

2 Haga clic en la pestaña Configurar.

3 En vSAN, haga clic en **Almacenes de datos remotos**.

4 Seleccione un almacén de datos remoto y haga clic en **Siguiente**.

5 Haga clic en **Desmontar** para confirmar.

Resultados

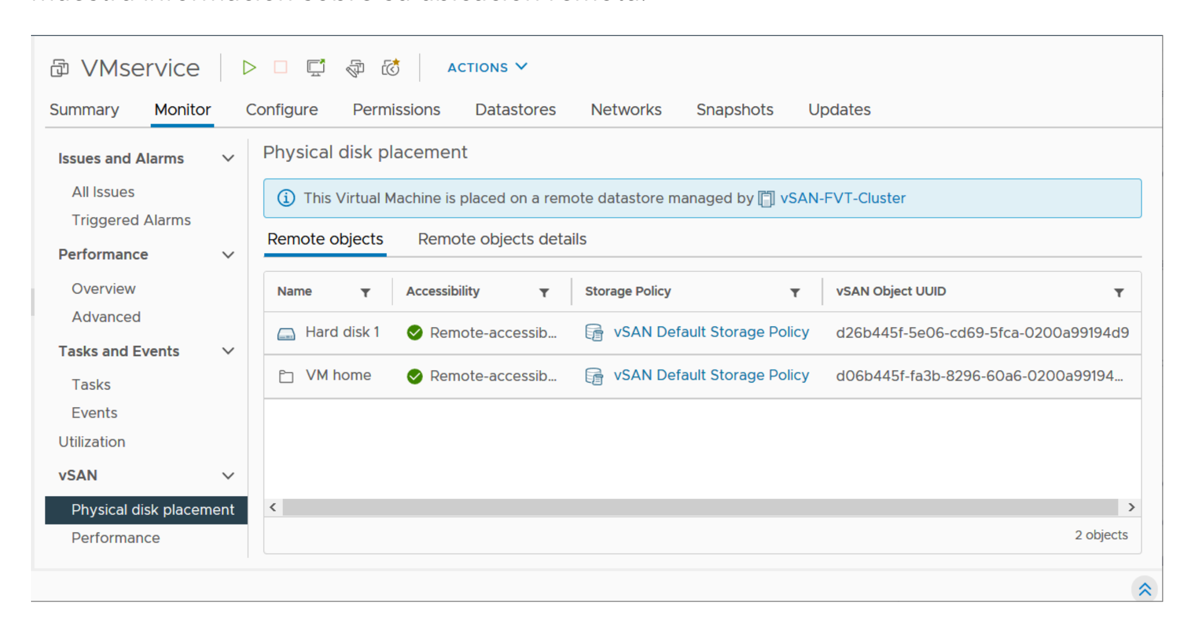
El almacén de datos seleccionado se desmontará del clúster local.

Supervisar el uso compartido de almacenes de datos con vSphere Client

Puede utilizar vSphere Client para supervisar el estado de las operaciones de uso compartido de almacenes de datos de vSAN.

El monitor de capacidad de vSAN le notifica cuando hay almacenes de datos remotos montados en el clúster. Puede seleccionar el almacén de datos remoto para consultar su capacidad.

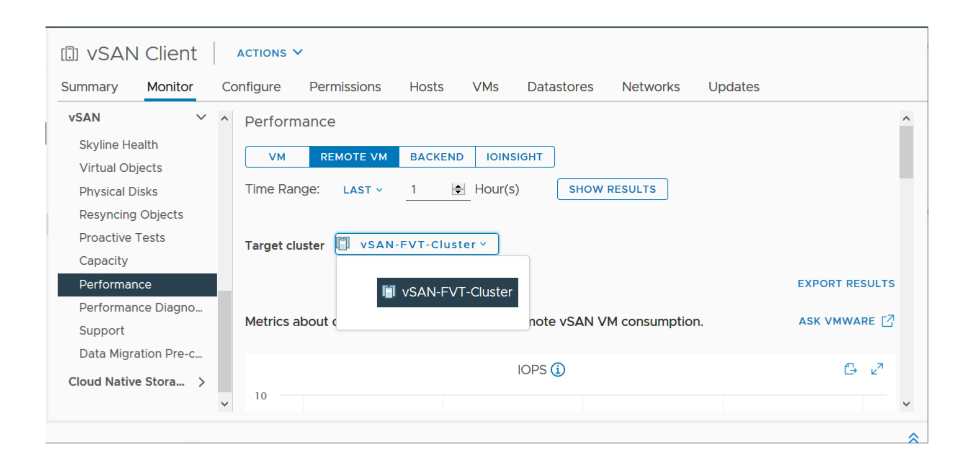
La vista Objetos virtuales muestra el almacén de datos en el que residen los objetos virtuales. La vista Colocación de discos físicos de una máquina virtual ubicada en un almacén de datos remoto muestra información sobre su ubicación remota.



Las comprobaciones de estado de vSAN indican el estado de las funciones de HCI.

- La comprobación Datos > Estado de objetos de vSAN muestra información de accesibilidad de los objetos remotos.
- La comprobación Red > Partición de clúster de servidores muestra las particiones de red entre los hosts del clúster de cliente y el clúster de servidores.
- La comprobación Red > Latencia comprueba la latencia entre los hosts del clúster de clientes y el clúster de servidores.

las vistas de rendimiento del clúster de vSAN incluyen gráficos de rendimiento de máquinas virtuales que muestran el rendimiento de cada máquina virtual del clúster cliente desde la perspectiva del clúster remoto. Puede seleccionar un almacén de datos remoto para ver el rendimiento.



Puede ejecutar pruebas proactivas en almacenes de datos remotos para comprobar la creación de máquinas virtuales y el rendimiento de la red. La prueba de creación de máquinas virtuales crea una máquina virtual en el almacén de datos remoto. La prueba de rendimiento de red comprueba el rendimiento de la red entre todos los hosts del clúster cliente y todos los hosts de los clústeres de servidores.

Agregar una instancia remota de vCenter como origen de almacén de datos

Puede agregar una instancia remota de vCenter como origen de almacén de datos remoto para los clientes en la instancia local de vCenter.

Procedimiento

1 Desplácese hasta vCenter en vSphere Client.

2 Seleccione **Configurar > vSAN > Almacenes de datos remotos**.

3 En la pestaña Orígenes de almacenes de datos, haga clic en **Agregar origen de almacén de datos remoto** para abrir el asistente.

4 Introduzca la información para especificar la instancia remota de vCenter.

5 Compruebe la compatibilidad, revise la configuración y haga clic en **Finalizar**.

Resultados

La instancia remota de vCenter se agregará como origen del almacén de datos. Los clústeres de vSAN en esta instancia de vCenter pueden montar almacenes de datos remotos que residen en la instancia remota de vCenter.

Trabajar con miembros del clúster de vSAN en modo de mantenimiento

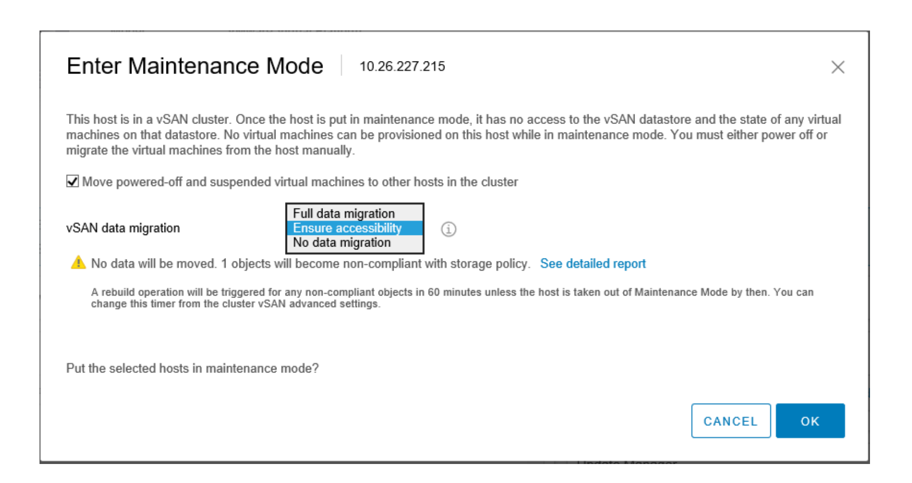
Antes de apagar, reiniciar o desconectar un host que es miembro de un clúster de vSAN, debe poner el host en modo de mantenimiento.

Al trabajar con el modo de mantenimiento, tenga en cuenta las siguientes directrices:

- Cuando coloque un host ESXi en el modo de mantenimiento, deberá seleccionar un modo de evacuación de datos, como **Garantizar disponibilidad** o **Migración de datos completa**.
- Cuando cualquier host miembro de un clúster de vSAN entra en modo de mantenimiento, la capacidad del clúster se reduce de manera automática, ya que el host miembro deja de aportar almacenamiento al clúster.
- Es posible que los recursos informáticos de una máquina virtual no estén en el host que se va a colocar en el modo de mantenimiento, y los recursos de almacenamiento de las máquinas virtuales pueden estar ubicados en cualquier parte del clúster.
- El modo **Garantizar disponibilidad** es más rápido que el modo **Migración de datos completa**, ya que **Garantizar disponibilidad** solo migra los componentes de los hosts que son imprescindibles para la ejecución de las máquinas virtuales. En este modo, si se experimenta un error, se ve afectada la disponibilidad de la máquina virtual. Cuando se selecciona el modo **Garantizar disponibilidad**, los datos no se reprotegen durante un error y puede experimentarse una pérdida de datos inesperada.
- Cuando se selecciona el modo **Migración de datos completa**, los datos se reprotegen automáticamente contra errores, si hay recursos disponibles y **Errores que se toleran** está establecido en 1 o más. En este modo, se migran todos los componentes del host y, según la cantidad de datos que haya en el host, es posible que la migración tarde más. En el modo **Migración de datos completa**, las máquinas virtuales pueden tolerar errores, incluso durante el mantenimiento planificado.
- Al trabajar con un clúster de tres hosts, no puede colocar un servidor en el modo de mantenimiento con **Migración de datos completa**. Para obtener la disponibilidad máxima, debe considerar la posibilidad de diseñar un clúster con cuatro hosts o más.

Antes de colocar un host en el modo de mantenimiento, debe comprobar lo siguiente:

- Si utiliza el modo **Migración de datos completa**, compruebe que el clúster disponga de suficientes hosts y capacidad disponible para cumplir con los requisitos de la directiva **Errores que se toleran**.
- Compruebe que exista suficiente capacidad flash en los hosts restantes para controlar las reservas de Flash Read Cache. Ejecute el comando de RVC `vsan.whatif_host_failures` para analizar el uso de capacidad actual por host y determinar si un único error de host podría causar que se agote el espacio del clúster y afectar la capacidad del clúster, la reserva de memoria caché y los componentes del clúster. Para obtener información sobre los comandos de RVC, consulte la *Guía de referencia de los comandos de RVC*.
- Verifique que disponga de suficientes dispositivos de capacidad en los hosts restantes para controlar los requisitos de la directiva de ancho de las fracciones, si está seleccionada.
- Asegúrese de disponer de suficiente capacidad libre en los hosts restantes para controlar la cantidad de datos que deben migrarse desde el host que va a entrar en modo de mantenimiento.



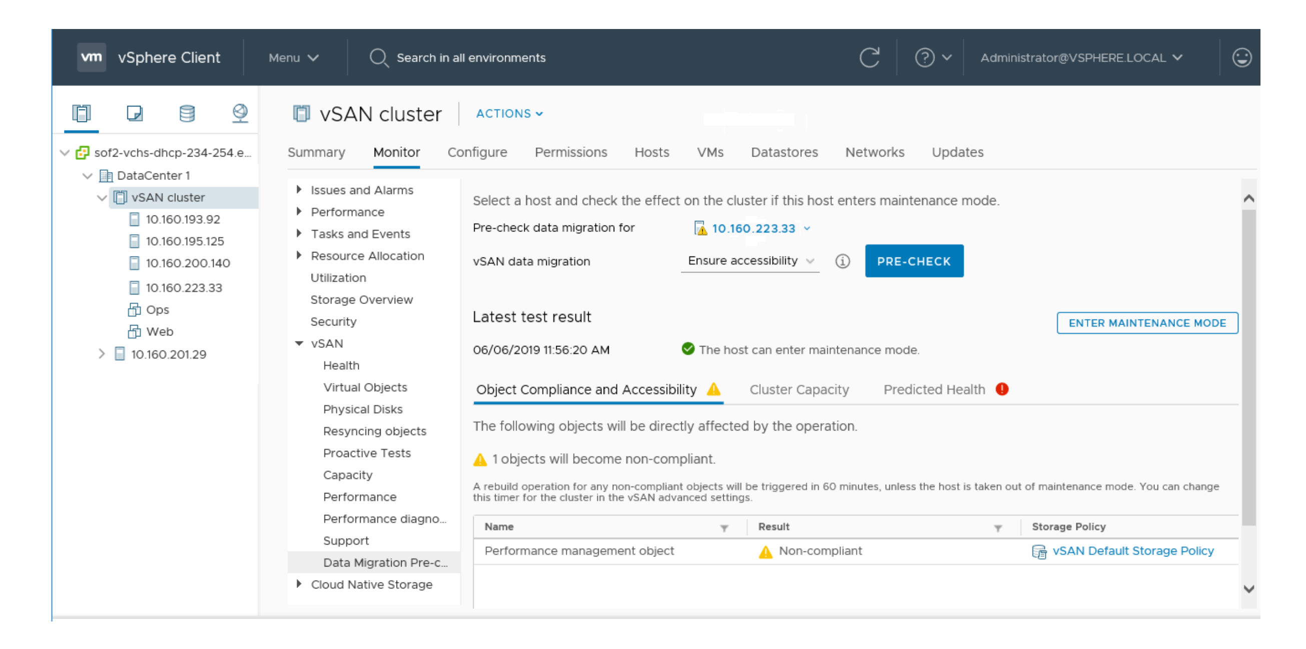
En el cuadro de diálogo Confirmar modo de mantenimiento se proporciona información para guiarle durante las actividades de mantenimiento. Puede ver el impacto de cada opción de evacuación de datos.

- Si hay o no suficiente capacidad para realizar la operación.
- Cuántos datos se moverán.
- Cuántos objetos dejarán de cumplir con las normas.
- Cuántos objetos se volverán inaccesibles.

Comprobar las capacidades de migración de datos de un host en el clúster de vSAN

Utilice la comprobación previa de migración de datos para identificar el impacto de las opciones de migración al poner un host en modo de mantenimiento o quitarlo del clúster.

Antes de poner un host de vSAN en modo de mantenimiento, ejecute la comprobación previa de migración de datos. Los resultados de la prueba proporcionarán información para determinar el impacto sobre la capacidad del clúster, las comprobaciones de estado previsto y los objetos que se apartarán del cumplimiento. Si se espera que la operación no se realice correctamente, la comprobación previa proporcionará información sobre los recursos necesarios.



Procedimiento

1 Desplácese hasta el clúster de vSAN.

2 Haga clic en la pestaña Supervisar.

3 En vSAN, haga clic en **Comprobación previa a la migración de datos**.

4 Seleccione un host, una opción de migración de datos y haga clic en **Comprobación previa**.

   vSAN ejecutará las pruebas de comprobación previa de migración de datos.

5 Vea los resultados de la prueba.

   Los resultados de la comprobación previa muestran si el host puede entrar en modo de mantenimiento de forma segura.

   - La pestaña Conformidad y accesibilidad de objetos muestra los objetos que pueden presentar problemas después de la migración de datos.
   - La pestaña Capacidad del clúster muestra el impacto de la migración de datos en el clúster de vSAN antes y después de realizar la operación.
   - La pestaña Estado previsto muestra las comprobaciones de estado que podrían verse afectadas por la migración de datos.

Pasos siguientes

Si la comprobación previa indica que puede poner el host en modo de mantenimiento, puede hacer clic en **Entrar en modo de mantenimiento** para migrar los datos y poner el host en modo de mantenimiento.

Poner un miembro de un clúster de vSAN en modo de mantenimiento

Antes de apagar, reiniciar o desconectar un host que es miembro de un clúster de vSAN, debe poner el host en modo de mantenimiento.

Cuando coloque un host en el modo de mantenimiento, deberá seleccionar un modo de evacuación de datos, como **Garantizar accesibilidad** o **Migración de datos completa**. Cuando cualquier host miembro de un clúster de vSAN entra en modo de mantenimiento, la capacidad del clúster se reduce de manera automática, ya que el host miembro deja de aportar capacidad al clúster.

Nota Las máquinas virtuales del servicio de archivos (FSVM) de vSAN que se ejecutan en un host se apagan automáticamente cuando un host del clúster de vSAN entra en modo de mantenimiento.

Todos los destinos de iSCSI de vSAN atendidos por este host se transfieren a otros hosts del clúster y, por tanto, el iniciador iSCSI se redirecciona al nuevo propietario de destino.

Requisitos previos

Compruebe que el entorno cuente con las funcionalidades necesarias para la opción seleccionada.

Procedimiento

1 Haga clic con el botón derecho en el host y seleccione **Maintenance Mode > Enter Maintenance Mode** (Modo de mantenimiento > Entrar en modo de mantenimiento).

2 Seleccione un modo de evacuación de datos y haga clic en **Aceptar**.

Opción	Descripción
Garantizar accesibilidad	Esta es la opción predeterminada. Cuando el host del clúster desconecta o se quita, vSAN migra solo suficientes datos para garantizar que se pueda acceder a todos los objetos una vez que el host entre en modo de mantenimiento. Seleccione esta opción si desea quitar el host temporalmente del clúster, por ejemplo, para instalar actualizaciones, y tiene planificado restituir el host en el clúster. Esta opción no es adecuada si se pretende quitar el host del clúster de manera permanente. Por lo general, solamente se requiere una evacuación parcial de datos. Sin embargo, es posible que la máquina virtual ya no cumpla por completo con la directiva de almacenamiento de la máquina virtual durante la evacuación. Eso significa que es posible que no tenga acceso a todas las réplicas. Si se produce un error mientras el host está en modo de mantenimiento y **Errores que se toleran** se establece como 1, es posible que se experimente una pérdida de datos en el clúster. **Nota** Este es el único modo de evacuación disponible si se trabaja con un clúster de tres hosts o con un clúster de vSAN configurado con tres dominios de errores.
Migración de datos completa	vSAN evacua todos los datos a otros hosts del clúster y mantiene el estado actual de cumplimiento de objetos. Seleccione esta opción si tiene planificado migrar el host de manera permanente. Al evacuar datos del último host del clúster, asegúrese de migrar las máquinas virtuales a otro almacén de datos y luego ponga el host en modo de mantenimiento. Este modo de evacuación genera el mayor volumen de transferencia de datos y consume más tiempo y recursos. Todos los componentes en el almacenamiento local del host seleccionado se migran a otra ubicación del clúster. Cuando el host entra en modo de mantenimiento, todas las máquinas virtuales pueden acceder a los componentes de almacenamiento y siguen cumpliendo con las directivas de almacenamiento que tienen asignadas. **Nota** Si hay objetos en estado de disponibilidad reducida, este modo mantiene este estado de cumplimiento y no garantiza que los objetos pasen a cumplir los requisitos. Si no es posible acceder a un objeto de máquina virtual que tiene datos en el host y no se evacua por completo, el host no podrá entrar en el modo de mantenimiento.
Sin migración de datos	vSAN no evacúa datos de este host. Al apagar el host o quitarlo del clúster, es posible que algunas máquinas virtuales dejen de estar accesibles.

Un clúster con tres dominios de errores tiene las mismas restricciones que un clúster con hosts, entre ellas, la imposibilidad de usar el modo **Migración de datos completa** o de reproteger los datos después de un error.

Como alternativa, puede poner un host en modo de mantenimiento mediante ESXCLI. Antes de poner un host en este modo, asegúrese de apagar las máquinas virtuales que se ejecutan en el host.

Para realizar una acción antes de entrar en modo de mantenimiento, ejecute el siguiente comando en el host:

```
esxcli system maintenanceMode set --enable 1 --vsanmode=<str>
```

A continuación se muestran los valores de cadena permitidos para vsanmode:

- ensureObjectAccessibility: los datos del disco se evacúan para garantizar la accesibilidad de los objetos en el clúster de vSAN antes de entrar en modo de mantenimiento.

  Nota El valor predeterminado es ensureObjectAccessibility. Este valor se utilizará si no especifica ningún valor para el vsanmode.

- evacuateAllData : todos los datos del disco se evacúan antes de entrar en modo de mantenimiento.
- noAction: los datos de vSAN no se mueven fuera del disco antes de entrar en modo de mantenimiento.

Para verificar el estado del host, ejecute el siguiente comando:

```
esxcli system maintenanceMode get
```

Para salir del modo de mantenimiento, ejecute el siguiente comando:

```
esxcli system maintenanceMode set --enable 0
```

Pasos siguientes

Puede hacer un seguimiento del progreso de la migración de datos en el clúster. Para obtener más información, consulte *Supervisión y solución de problemas de vSAN*.

Administrar dominios de errores en clústeres de vSAN

Los dominios de errores son una protección contra los errores en el bastidor o el chasis si el clúster de vSAN abarca varios bastidores o chasis de servidores blade.

Puede crear dominios de errores y agregar uno o varios hosts a cada dominio de errores. Un dominio de errores consta de uno o varios hosts de vSAN agrupados según su ubicación física en el centro de datos. Cuando se configuran, los dominios de errores permiten que vSAN tolere errores de bastidores físicos completos, así como errores de un único host, un dispositivo de capacidad, un vínculo de red o un conmutador de red dedicado a un dominio de errores.

La directiva **Errores que se toleran** depende de la cantidad de errores que una máquina virtual se aprovisionó para tolerar. Cuando se configura una máquina virtual con **Errores que se toleran** establecido como 1 `(FTT=1)`, vSAN puede tolerar un solo error de cualquier tipo y de cualquier componente en un dominio de errores, incluidos errores en un bastidor completo.

Cuando se configuran dominios de errores en un bastidor y se aprovisiona una máquina virtual nueva, vSAN garantiza que los objetos de protección como las réplicas y los testigos se ubiquen en dominios de errores diferentes. Por ejemplo, si la directiva de almacenamiento de una máquina virtual tiene el atributo **Errores que se toleran** establecido en N `(FTT=n)`, vSAN requiere un mínimo de `2*n+1` dominios de errores en el clúster. Cuando se aprovisionan máquinas virtuales en un clúster con dominios de errores que usan esta directiva, las copias de los objetos asociados de máquinas virtuales se almacenan en bastidores separados.

Se requieren al menos tres dominios de errores para admitir que FTT sea igual a 1. Para obtener mejores resultados, configure cuatro dominios de errores o más en el clúster. Un clúster con tres dominios de errores tiene las mismas restricciones que un clúster con hosts, entre ellas, la imposibilidad de reproteger datos después de un error y de usar el modo **Full data migration** (Migración de datos completa). Para obtener información sobre cómo diseñar dominios de errores y definir su tamaño, consulte "Diseñar dominios de errores de vSAN y definir su tamaño" en *Planificar e implementar vSAN*.

Piense en un escenario en el cual tiene un clúster de vSAN con 16 hosts. Los hosts se distribuyen entre cuatro bastidores (es decir, cuatro hosts por bastidor). Para tolerar errores en un bastidor completo, cree un dominio de errores para cada bastidor. Puede configurar un clúster con esa capacidad con **Errores que se toleran** establecido como 1. Si desea establecer **Errores que se toleran** como 2, configure cinco dominios de errores en el clúster.

Cuando se produce un error en un bastidor, todos los recursos, incluida la CPU y la memoria en el bastidor, dejan de estar disponibles en el clúster. Para reducir el impacto de un posible error de bastidor, configure dominios de errores de menor tamaño. Al aumentar el número de dominios de errores, la cantidad total de recursos disponibles aumenta en el clúster después de un error de bastidor.

Al trabajar con dominios de errores, siga las prácticas recomendadas.

- Configure un mínimo de tres dominios de errores en el clúster de vSAN. Para obtener mejores resultados, configure cuatro dominios de errores.
- Un host que no forma parte de ningún dominio de errores se considera que reside en su propio dominio de errores de host individual.
- No es necesario asignar cada host de vSAN a un dominio de errores. Si decide usar dominios de errores para proteger el entorno de vSAN, considere la posibilidad de crear dominios de errores del mismo tamaño.
- Cuando se transfieren a otro clúster, los hosts de vSAN retienen las asignaciones de dominios de errores.
- Al diseñar un dominio de errores, coloque una cantidad de hosts uniforme en cada dominio de errores.

  Para obtener instrucciones sobre el diseño de dominios de errores, consulte "Diseñar dominios de errores de vSAN y definir su tamaño" en *Planificar e implementar vSAN*.

- Puede agregar cualquier cantidad de hosts a un dominio de errores. Cada dominio de errores debe contener al menos un host.

Crear un nuevo dominio de errores en un clúster de vSAN

Para garantizar que los objetos de máquinas virtuales sigan ejecutándose correctamente durante un error de un bastidor, puede agrupar los hosts en distintos dominios de errores.

Al aprovisionar una máquina virtual en el clúster con dominios de errores, vSAN distribuye los componentes de protección, como los testigos y las réplicas de los objetos de máquinas virtuales entre distintos dominios de errores. Como consecuencia, el entorno de vSAN puede tolerar errores de bastidores completos, además de errores individuales en un host, en un disco de almacenamiento o en una red.

Requisitos previos

- Elija un nombre único para el dominio de errores. vSAN no admite nombres duplicados de dominios de errores en un clúster.
- Compruebe la versión de los hosts ESXi. Solamente puede incluir hosts de la versión 6.0 o posteriores en los dominios de errores.
- Compruebe que los hosts de vSAN estén conectados. No es posible asignar hosts a un dominio de errores que está sin conexión o que no está disponible debido a un problema de configuración del hardware.

Procedimiento

1. Desplácese hasta el clúster de vSAN.
2. Haga clic en la pestaña **Configurar**.
3. En vSAN, haga clic en **Dominios de errores**.
4. Haga clic en el icono más. Se abrirá el asistente Nuevo dominio de errores.
5. Introduzca el nombre del dominio de errores.
6. Seleccione un host o más para agregar al dominio de errores.

   Un dominio de errores no puede estar vacío. Debe seleccionar al menos un host para incluir en el dominio de errores.
7. Haga clic en **Crear**.

   Los hosts seleccionados se muestran en el dominio de errores. Cada dominio de errores muestra información de la capacidad utilizada y reservada. Esto permite ver la distribución de la capacidad en el dominio de errores.

Transferir hosts al dominio de errores seleccionado en un clúster de vSAN

Puede transferir un host a un dominio de errores seleccionado en el clúster de vSAN.

Procedimiento

1 Desplácese hasta el clúster de vSAN.

2 Haga clic en la pestaña **Configurar**.

3 En vSAN, haga clic en **Dominios de errores**.

4 Seleccione y arrastre el host que desea agregar a un dominio de errores existente.

   El host seleccionado aparecen en el dominio de errores.

Transferir hosts fuera de un dominio de errores en un clúster de vSAN

Según sus requisitos, puede transferir hosts fuera del dominio de errores.

Requisitos previos

Compruebe que el host esté en línea. No puede mover hosts que están sin conexión o no están disponibles en un dominio de errores.

Procedimiento

1 Desplácese hasta el clúster de vSAN.

2 Haga clic en la pestaña **Configurar**.

3 En vSAN, haga clic en **Dominios de errores**.

   a Seleccione y arrastre el host desde el dominio de errores hacia el área Hosts independientes.

   b Haga clic en **Mover** para confirmar.

Resultados

El host seleccionado ya no forma parte del dominio de errores. Cualquier host que no forma parte de un dominio de errores se considera su propio dominio de errores de host individual.

Pasos siguientes

Puede agregar hosts a dominios de errores. Consulte Transferir hosts al dominio de errores seleccionado en un clúster de vSAN.

Cambiar el nombre de un dominio de errores en un clúster de vSAN

Puede cambiar el nombre de un dominio de errores existente en el clúster de vSAN.

Procedimiento

1 Desplácese hasta el clúster de vSAN.

2 Haga clic en la pestaña **Configurar**.

3 En vSAN, haga clic en **Dominios de errores**.

   a Haga clic en el icono Acciones en el lado derecho del dominio de errores y seleccione **Editar**.

   b Introduzca un nombre de dominio de errores.

4 Haga clic en **Aplicar** o en **Aceptar**.

   El nombre nuevo aparecerá en la lista de dominios de errores.

Quitar dominios de errores seleccionados de un clúster de vSAN

Cuando ya no necesita un dominio de errores, puede quitarlo del clúster de vSAN.

Procedimiento

1 Desplácese hasta el clúster de vSAN.

2 Haga clic en la pestaña **Configurar**.

3 En vSAN, haga clic en **Dominios de errores**.

4 Haga clic en el icono Acciones en el lado derecho del dominio de errores y seleccione **Eliminar**.

5 Haga clic en **Eliminar** para confirmar.

Resultados

Se quitan todos los hosts del dominio de errores y se elimina el dominio de errores seleccionado del clúster de vSAN. Se considera que cada host que no forma parte de un dominio de errores reside en su propio dominio de errores de host individual.

Tolerar errores adicionales con dominio de errores en un clúster de vSAN

Los dominios de errores en un clúster de vSAN ofrecen resistencia y garantizan que los datos estén disponibles incluso con errores basados en directivas.

Si se establece en 1 el número de errores que se toleran (FTT), el objeto podrá tolerar un error. Sin embargo, un error temporal seguido de un error permanente en un clúster puede provocar la pérdida de datos. Un dominio de errores adicional proporciona a vSAN la capacidad de crear un componente activo sin tener que aumentar el número de FTT para el objeto. vSAN activa este componente adicional durante errores planificados e imprevistos. Los errores no planificados incluyen la desconexiones de red, errores de disco y errores de host. Los errores planificados incluyen entrar en modo de mantenimiento (EMM). Por ejemplo, un clúster de 6 hosts con un objeto RAID 6 no puede crear un componente activo si se produce un error en el host.

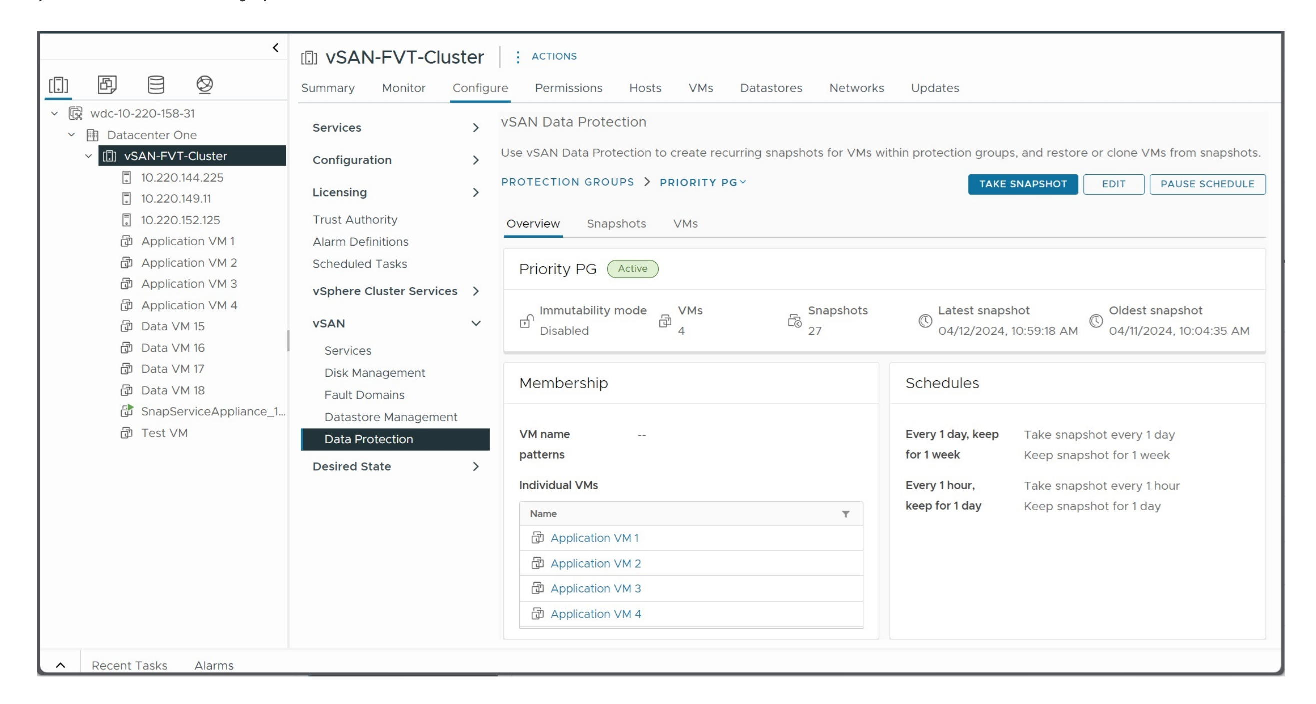
vSAN garantiza la disponibilidad de datos de los objetos cuando los componentes se desconectan y vuelven a conectarse de forma inesperada en función de los FTT especificados en la directiva de almacenamiento. Durante un error, las escrituras del componente con errores se redireccionan al componente activo. Cuando el componente se recupera del error transitorio y vuelve a estar conectado, el componente activo desaparece y se vuelve a sincronizar el componente.

Si el componente activo no está disponible y se produce un segundo error permanente en el clúster y el objeto reflejado se ve afectado, los datos del objeto se perderán de forma permanente aunque se resuelva el error.

Usar vSAN Data Protection

vSAN Data Protection permite recuperar rápidamente las máquinas virtuales ante errores operativos o ataques de ransomware mediante instantáneas nativas almacenadas de forma local en el clúster de vSAN.

vSAN Data Protection se admite en clústeres de vSAN HCI con vSAN ESA. Utiliza instantáneas de vSAN nativas para capturar el estado actual de las máquinas virtuales. Puede utilizar instantáneas de vSAN para restaurar una máquina virtual a su estado anterior o clonar una máquina virtual para desarrollo y pruebas.



vSAN Data Protection requiere el servicio de instantáneas de VMware para administrar instantáneas de vSAN. Implemente el dispositivo del servicio de instantáneas para habilitar vSAN Data Protection en vSphere Client.

Utilice las siguientes pestañas para desplazarse por la página de vSAN Data Protection.

Pestaña	Descripción
Resumen	Muestra información general sobre vSAN Data Protection, incluidos el número de grupos de protección, el porcentaje de máquinas virtuales protegidas, el número de instantáneas de máquinas virtuales y la cantidad de espacio de almacenamiento utilizado para las instantáneas.
Grupos de protección	Muestra una lista de grupos de vSAN Data Protection y su estado. Seleccione un grupo de protección para ver las instantáneas en dicho grupo de protección o edite la configuración.
Máquinas virtuales	Muestra una lista de las máquinas virtuales del clúster de vSAN con detalles sobre su estado de protección de datos. Aquí se pueden ver las máquinas virtuales eliminadas que tienen instantáneas disponibles. Puede seleccionar una máquina virtual y hacer clic para restaurarla o clonarla.

Instantáneas de vSAN

Las instantáneas de vSAN conservan el estado y los datos de una máquina virtual en el momento en el que se crea dicha instantánea. Este archivo local conserva los datos de la máquina virtual tal cual estaban en ese momento. Puede restaurar una máquina virtual al estado que existía cuando se tomó la instantánea o crear una máquina virtual de clon vinculado que coincida con el estado conservado en la instantánea.

Al crear una instantánea, se captura el estado de la máquina virtual en un momento específico. Las instantáneas de vSAN no se ponen en modo inactivo y capturan el estado de ejecución actual de la máquina virtual.

Las instantáneas funcionan en máquinas virtuales individuales. Cada máquina virtual requiere una instantánea independiente. Puede crear instantáneas manuales o programadas de máquinas virtuales colocándolas en grupos de protección.

Cada instantánea de vSAN contiene el estado del objeto de espacio de nombres de la máquina virtual y los objetos del disco virtual. vSAN crea instantáneas de las máquinas virtuales de los grupos de protección a intervalos programados. Estas instantáneas de vSAN se almacenan localmente en el almacén de datos de vSAN.

Grupos de protección

Los grupos de protección permiten programar y administrar instantáneas para una o varias máquinas virtuales. Puede agregar máquinas virtuales a un grupo de protección, configurar programaciones de instantáneas y ver información de instantáneas.

Seleccione un grupo de protección y utilice las siguientes pestañas para administrarlo.

Pestaña	Descripción
Descripción general	Muestra información general sobre el grupo de protección, incluida una lista de máquinas virtuales miembro, las programaciones de instantáneas y el número de instantáneas realizadas.
Instantáneas	Muestra la serie de instantáneas asociada con el grupo de protección. Puede seleccionar y eliminar instantáneas individuales de la serie.
Máquinas virtuales	Muestra una lista de máquinas virtuales que son miembros del grupo de protección, así como el número de instantáneas disponibles para cada máquina virtual.

Cuando cree un grupo de protección, agregue máquinas virtuales miembro y configure una o varias programaciones de instantáneas. Puede agregar máquinas virtuales de forma individual o introducir patrones de nombre para agregar todas las máquinas virtuales que coincidan con dicho patrón. Puede utilizar ambos métodos para agregar máquinas virtuales al grupo de protección.

Puede definir varias programaciones de instantáneas para capturar periódicamente el estado de las máquinas virtuales en un grupo de protección. A medida que se capturan nuevas instantáneas, vSAN elimina las instantáneas antiguas de la serie, según la configuración de retención. También puede crear una instantánea manual para capturar el estado actual de las máquinas virtuales en el grupo de protección.

Habilite el **modo de inmutabilidad** en un grupo de protección para mayor seguridad. No se puede editar o eliminar este grupo de protección, cambiar la pertenencia de la máquina virtual, ni editar o eliminar instantáneas. Una instantánea inmutable es una copia de solo lectura de datos que no se puede modificar ni eliminar, ni siquiera por un atacante con privilegios administrativos.

Nota Una vez habilitado el modo de inmutabilidad en un grupo de protección, los administradores no podrán deshabilitarlo.

Puede supervisar y modificar grupos de protección desde la pestaña Grupos de protección. Haga clic en un grupo de protección para ver sus detalles.

- En **Descripción general** se muestra información general sobre el grupo de protección, incluidos la pertenencia a máquinas virtuales, las programaciones de instantáneas y el número de instantáneas.
- En **Instantáneas** se muestra una lista de las instantáneas disponibles en el grupo de protección. Puede seleccionar una instantánea, hacer clic en **>>** para ver instantáneas individuales de cada máquina virtual y realizar acciones.
- En **Máquinas virtuales** se muestra una lista de las máquinas virtuales del grupo de protección con detalles sobre las instantáneas disponibles. Seleccione un botón de opción de máquina virtual y haga clic en **Restaurar máquina virtual** o **Clonar máquina virtual** y, a continuación, elija una instantánea.

Haga clic en uno de los siguientes botones para realizar acciones en el grupo de protección.

Acción	Descripción
Crear instantánea	Puede cambiar el nombre predeterminado de la instantánea y definir el período de retención. vSAN crea una instantánea independiente para cada máquina virtual del grupo de protección.
Editar	Puede agregar o eliminar máquinas virtuales, modificar los patrones de nombres de máquinas virtuales y agregar o modificar las programaciones de instantáneas.
Pausar programación/ Reanudar programación	Puede pausar las programaciones de instantáneas definidas para el grupo de protección. No se crearán ni eliminarán instantáneas mientras las programaciones estén pausadas.

Para eliminar un grupo de protección, haga clic en el icono **Más...** junto al nombre del grupo y seleccione el menú **Eliminar**. Al eliminar el grupo de protección, debe decidir cómo administrar sus instantáneas.

- **Conservar las instantáneas hasta su fecha de caducidad**. El grupo de protección se eliminará después de que hayan caducado todas sus instantáneas.
- **Eliminar instantáneas**. El grupo de protección y sus instantáneas se eliminarán inmediatamente.

vSAN y VMware Live Cyber Recovery

VMware Live Cyber Recovery puede aprovechar las instantáneas de vSAN en el sitio protegido para conseguir una recuperación más rápida de las máquinas virtuales infectadas por ransomware en la nube. VLCR puede reducir los tiempos de restauración usando las instantáneas de vSAN para actualizar solo los deltas de las máquinas virtuales en el sitio de producción.

Para obtener más información, consulte "Restauración rápida mediante instantáneas locales de VMware vSAN" en *VMware Live Cyber Recovery*.

Implementación del dispositivo del servicio de instantáneas

vSAN Data Protection requiere el dispositivo del servicio de instantáneas de VMware para administrar instantáneas de vSAN.

Implemente el dispositivo del servicio de instantáneas en el mismo sitio que vCenter con una conexión de red de baja latencia.

Descargue e implemente el archivo OVA para agregar el dispositivo del servicio de instantáneas de VMware. Implementar un archivo OVA de dispositivo es similar a implementar una máquina virtual desde una plantilla.

Este dispositivo requiere un certificado de vCenter Server de confianza. En la página de inicio de vCenter, haga clic en **Descargar certificados de CA raíz de confianza**. Extraiga los archivos de certificado, abra **Certs > lin** y copie el texto del archivo con la extensión .0. Puede consultar instrucciones detalladas en el siguiente artículo de la base de conocimientos: https://knowledge.broadcom.com/external/article/330833/how-to-download-and-install-vcenter-serv.html

Procedimiento

1. Descargue el dispositivo del servicio de instantáneas de VMware del sitio web de Broadcom en https://support.broadcom.com/group/ecx/downloads.
2. Haga clic con el botón secundario en el clúster de vSAN en vSphere Client y seleccione **Implementar plantilla de OVF** para abrir el asistente.
3. En la página **Seleccione una plantilla de OVF**, especifique la ubicación del archivo OVA de dispositivo y haga clic en **Siguiente**.

4 En la página **Seleccionar un nombre y una carpeta**, puede introducir un nombre único para el dispositivo, seleccionar su centro de datos como ubicación de la implementación.

5 En la página **Seleccionar recurso informático**, seleccione el clúster de vSAN como el recurso informático.

6 En la página **Seleccionar almacenamiento**, seleccione un almacén de datos.

7 En la página **Seleccionar redes**, seleccione la misma red que vCenter y haga clic en **Siguiente**.

8 En la página **Personalizar plantilla**, introduzca la contraseña raíz de la máquina virtual del dispositivo y especifique la instancia de vCenter en la que desea implementar el dispositivo. En el campo **Certificado de vCenter Server**, introduzca el texto del certificado.

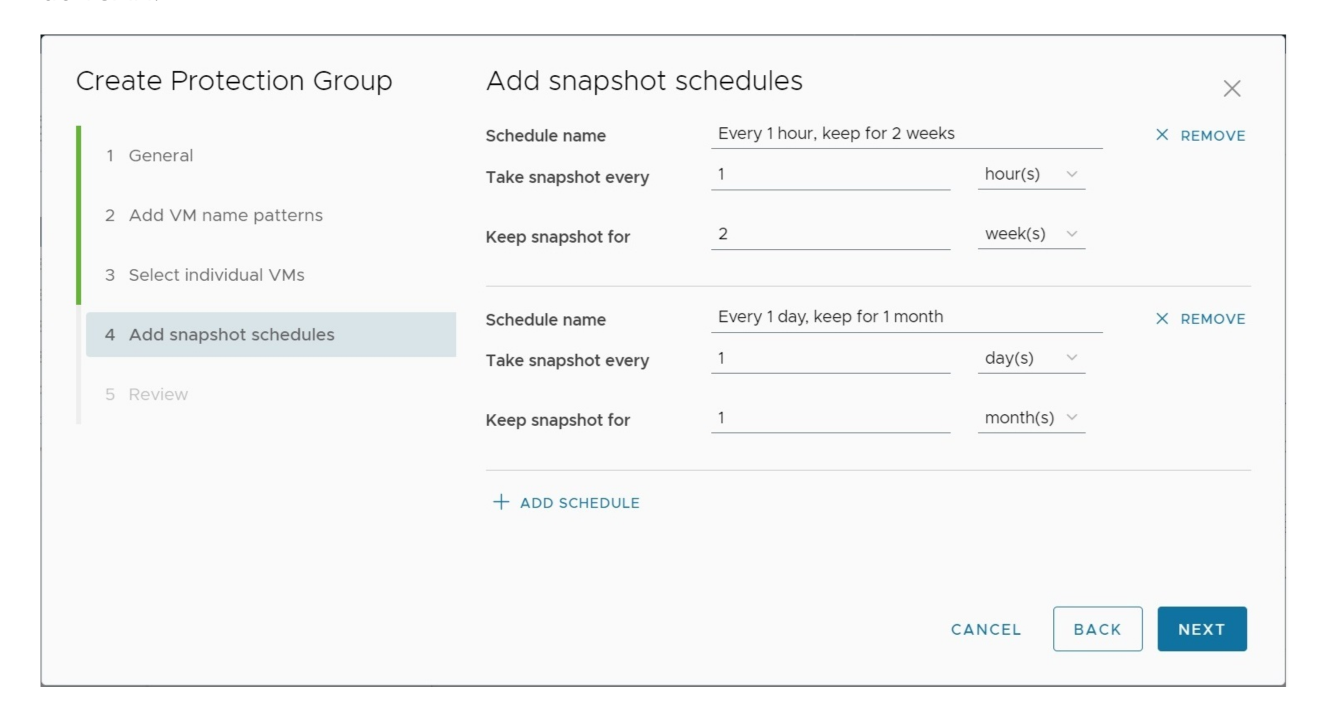
Resultados

El servicio de instantáneas de VMware se implementará en la instancia de vCenter especificada, y las páginas de vSAN Data Protection pasarán a estar disponibles en vSphere Client.

Crear un grupo de vSAN Data Protection

Coloque las máquinas virtuales en un grupo de protección de datos para programar y administrar instantáneas de forma coherente para todas las máquinas virtuales que sean miembros del grupo.

Los grupos de protección permiten programar y administrar instantáneas de vSAN para una o varias máquinas virtuales. No puede agregar máquinas virtuales de clones vinculados ni máquinas virtuales que tengan instantáneas de vSphere de un grupo de protección de datos de vSAN.



Requisitos previos

Asegúrese de que su clúster de vSAN cumple los siguientes requisitos:

- vSAN Express Storage Architecture
- vSAN 8.0 Update 3 o una versión posterior
- Dispositivo del servicio de instantáneas de VMware implementado en vCenter

Procedimiento

1. Desplácese hasta un clúster de vSAN en vSphere Client.
2. Haga clic en la pestaña Configurar y seleccione **vSAN > Protección de datos**.
3. Seleccione Grupos de protección y haga clic en **Crear grupo de protección** para abrir el asistente.

   a. En la página General, introduzca un nombre para el grupo de protección y elija cómo definir la pertenencia a la máquina virtual.

   > **Nota** Habilite el modo de inmutabilidad para crear instantáneas de solo lectura que no se puedan modificar ni eliminar, ni siquiera por un atacante con privilegios administrativos. Una vez habilitado el modo de inmutabilidad, los administradores no podrán deshabilitarlo.

   b. (Opcional) En la página **Agregar patrones de nombres de máquinas virtuales**, introduzca uno o varios patrones de nombre de máquina virtual para que coincidan.

   Todas las máquinas virtuales del clúster cuyo nombre coincida con el patrón se agregarán al grupo de protección. Utilice caracteres especiales para definir cada patrón de nombre de máquina virtual.

   - Use * para que coincida con cero o más caracteres. Por ejemplo, los patrones de nombres de máquinas virtuales *database** y *prod-*-x* coincidirían con las máquinas virtuales "databaseSQL", "prod-1-x" y "prod-23-x".
   - Use ? para que coincida exactamente con un carácter. Por ejemplo, el patrón de nombre de máquina virtual *prod-?* coincidirá con la máquina virtual "prod-1", pero no con "prod-23"

   c. (Opcional) En la página **Seleccionar máquinas virtuales individuales**, seleccione las máquinas virtuales de la lista que desee agregar como miembros del grupo de protección.

d En la página **Agregar programaciones de instantáneas**, defina las programaciones de instantáneas y los intervalos de retención.

   Puede agregar hasta 10 programaciones de instantáneas. Introduzca un nombre para la programación y seleccione la frecuencia con la que vSAN debe crear instantáneas de las máquinas virtuales del grupo de protección. Seleccione durante cuánto tiempo desea conservar las instantáneas programadas.

e En la página Revisar, revise la selección y haga clic en **Crear**.

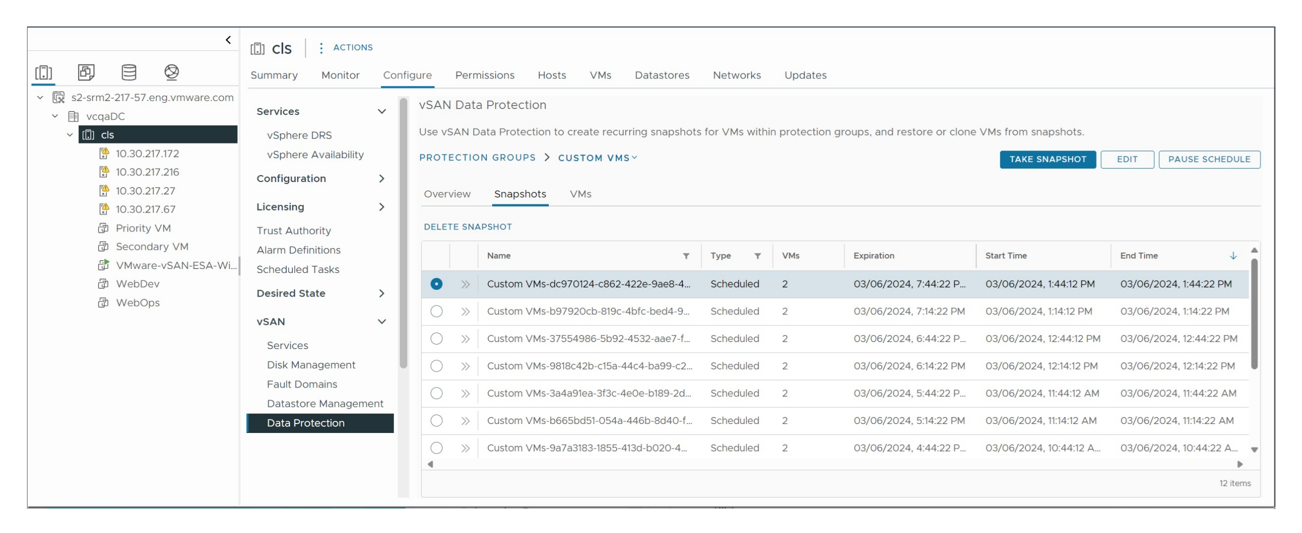
Pasos siguientes

Puede editar la configuración del grupo de protección. Puede crear una instantánea manual para capturar el estado actual de las máquinas virtuales en el grupo de protección.

Eliminar instantáneas de vSAN

Utilice vSphere Client para eliminar instantáneas de vSAN de un grupo de protección.

Seleccione instantáneas de vSAN en un grupo de protección y elimine las instantáneas del grupo.



Procedimiento

1 Desplácese hasta el clúster de vSAN en vSphere Client y seleccione **Configurar > vSAN > Protección de datos**.

2 Seleccione la pestaña **Grupos de protección**, haga clic en un grupo de protección y seleccione la pestaña Instantáneas.

3 Seleccione una instantánea y haga clic en **Eliminar instantánea**.

4 Haga clic en **Eliminar**.

Restaurar una máquina virtual a partir de una instantánea de vSAN

Puede utilizar una instantánea de vSAN para restaurar una máquina virtual al estado anterior conservado en la instantánea.

Cuando se restaura una máquina virtual a partir de una instantánea de vSAN, vSAN reemplaza la máquina virtual actual por la máquina virtual de la instantánea. Puede restaurar una máquina virtual eliminada que tenga instantáneas disponibles.

Procedimiento

1 Haga clic con el botón secundario en una máquina virtual en vSphere Client y seleccione el menú **Instantáneas > vSAN Data Protection > Administración de instantáneas**.

   Para buscar instantáneas de una máquina virtual retirada o eliminada, vaya a la página Configurar > vSAN > Protección de datos, haga clic en la pestaña **Máquinas virtuales** y, a continuación, seleccione **Máquinas virtuales eliminadas**.

2 Seleccione una instantánea de la lista y haga clic en **Restaurar máquina virtual**.

3 En el cuadro de diálogo Restaurar, haga clic en **Restaurar** para realizar la operación.

   La máquina virtual se desconectará y se creará una nueva instantánea para capturar el estado actual de la máquina virtual, de modo que pueda revertir a ella si es necesario.

Resultados

La máquina virtual se restaurará al estado anterior especificado por la instantánea.

Clonar una máquina virtual a partir de una instantánea de vSAN

Puede utilizar una instantánea de vSAN para crear una máquina virtual de clon vinculado que coincida con el estado de la máquina virtual original.

Al clonar una máquina virtual a partir de una instantánea de vSAN, deberá especificar la ubicación y el recurso informático del clon.

Procedimiento

1 Haga clic con el botón secundario en una máquina virtual en vSphere Client y seleccione el menú **Instantáneas > vSAN Data Protection > Administración de instantáneas**.

2 Seleccione una instantánea de la lista y haga clic en **Clonar máquina virtual** para abrir el cuadro de diálogo Clonar máquina virtual.

3 Introduzca un nombre para el clon, seleccione una ubicación y haga clic en **Siguiente**.

4 Seleccione el recurso informático para el clon y haga clic en **Siguiente**.

5 Revise la información y haga clic en **Clonar**.

Resultados

Se creará la máquina virtual de clon vinculado, que estará disponible en vCenter.

Usar el servicio del destino iSCSI de vSAN

Use el servicio del destino iSCSI para habilitar los hosts y las cargas de trabajo físicas que se encuentren fuera del clúster de vSAN para acceder al almacén de datos de vSAN.

Esta característica permite que un iniciador iSCSI en un host remoto transporte datos a nivel de bloque a un destino iSCSI en un dispositivo de almacenamiento del clúster de vSAN. vSAN 6.7 y las versiones posteriores admiten los clústeres de conmutación por error de Windows Server (WSFC), de modo que los nodos de WSFC pueden acceder a destinos de iSCSI de vSAN.

Tras configurar el servicio del destino iSCSI de vSAN, podrá detectar los destinos iSCSI de vSAN desde un host remoto. Para detectar destinos iSCSI de vSAN, use el puerto TCP del destino iSCSI y la dirección IP de cualquier host del clúster de vSAN. Para garantizar la alta disponibilidad del destino iSCSI de vSAN, configure el soporte de múltiples rutas para la aplicación iSCSI. Puede usar las direcciones IP de dos o más hosts para configurar múltiples rutas.

Nota El servicio del destino iSCSI de vSAN no admite otros clientes o iniciadores de vSphere o ESXi, hipervisores de terceros ni migraciones que usen asignaciones de dispositivos sin formato (raw device mapping, RDM).

El servicio del destino iSCSI de vSAN admite los siguientes métodos de autenticación de CHAP:

CHAP

En la autenticación de CHAP, el destino autentica el iniciador, pero el iniciador no autentica el destino.

CHAP mutuo

En la autenticación de CHAP mutuo, un nivel extra de seguridad permite que el iniciador autentique el destino.

Para obtener más información sobre el uso del servicio del destino iSCSI de vSAN, consulte la *Guía de uso del destino iSCSI* https://core.vmware.com/resource/vsan-iscsi-target-usage-guide.

Destinos iSCSI

Puede agregar uno o más destinos iSCSI que proporcionen bloques de almacenamiento como números de unidad lógica (logical unit number, LUN). vSAN identifica cada destino iSCSI con un nombre completo de iSCSI (iSCSI qualified Name, IQN) único. Puede usar el IQN para presentar el destino iSCSI a un iniciador iSCSI remoto de modo que este pueda acceder al LUN del destino.

Cada destino iSCSI contiene uno o más LUN. En un clúster de vSAN se define el tamaño de cada LUN, se asigna una directiva de almacenamiento de vSAN a cada LUN y se habilita el servicio del destino iSCSI. Puede configurar una directiva de almacenamiento para usarla como directiva predeterminada del objeto de inicio del servicio del destino iSCSI de vSAN.

Grupos de iniciadores iSCSI

Puede definir un grupo de iniciadores iSCSI que tengan acceso a un destino iSCSI concreto. El grupo de iniciadores iSCSI solo permitirá el acceso de aquellos iniciadores que sean miembros del grupo. Si no define un iniciador o un grupo de iniciadores iSCSI, los iniciadores iSCSI podrán acceder a todos los destinos.

Un nombre único identifica a cada grupo de iniciadores iSCSI. Puede agregar uno o más iniciadores iSCSI como miembros del grupo. Use el IQN del iniciador como nombre del iniciador del miembro.

Habilitar el servicio del destino iSCSI de vSAN

Antes de crear destinos y LUN iSCSI y definir grupos de iniciadores iSCSI, debe habilitar el servicio del destino iSCSI en el clúster de vSAN.

Procedimiento

1 Desplácese hasta el clúster de vSAN y haga clic en **Configurar** > **vSAN** > **Servicios**.

2 En el servicio del destino iSCSI de vSAN, haga clic **HABILITAR**.

   Se abrirá el asistente Editar el servicio del destino iSCSI de vSAN.

3 Edite la configuración del servicio de destino iSCSI de vSAN.

   Ahora es cuando se pueden seleccionar la red predeterminada, el puerto TCP y el método de autenticación. También puede seleccionar una directiva de almacenamiento de vSAN.

4 Haga clic en el control deslizante **Habilitar el servicio del destino iSCSI de vSAN** para activarlo y, a continuación, en **APLICAR**.

Resultados

El servicio del destino iSCSI de vSAN quedará habilitado.

Pasos siguientes

Tras habilitar el servicio del destino iSCSI, podrá crear destinos y LUN iSCSI, así como definir grupos de iniciadores iSCSI.

Crear un destino iSCSI de vSAN

Puede crear o editar un destino iSCSI y su LUN asociado.

Requisitos previos

Compruebe que el servicio del destino iSCSI de vSAN esté habilitado.

Procedimiento

1 Desplácese hasta el clúster de vSAN.

2 Haga clic en la pestaña **Configurar**.

   a En vSAN, haga clic en **Servicio del destino iSCSI**.

   b Haga clic en la pestaña Destinos iSCSI.

   c Haga clic en **Agregar**. Se abrirá el cuadro de diálogo **Nuevo destino iSCSI**. Si deja en blanco el campo IQN de destino, el IQN se generará automáticamente.

   d Escriba un **Alias** para el destino.

e Seleccione una opción para **Directiva de almacenamiento**, **Red**, **Puerto TCP** y método de **Autenticación**.

f Seleccione la **Ubicación del propietario de E/S**. Esta función solo está disponible si ha configurado el clúster de vSAN como un clúster ampliado. Permite especificar la ubicación del sitio para alojar el servicio de destino iSCSI de un destino. Esto permitirá evitar el tráfico de iSCSI entre sitios. Si ha establecido la directiva como HFT>=1, en caso de que se produzca un error en el sitio, la ubicación del propietario de E/S cambiará al sitio alternativo. Después de la recuperación de errores del sitio, la ubicación del propietario de E/S vuelve a cambiar automáticamente a la ubicación original del propietario de E/S según la configuración. Puede seleccionar una de las siguientes opciones para establecer la ubicación del sitio:

- **Cualquiera**: aloja el servicio del destino iSCSI tanto en el sitio preferido como en el secundario.
- **Preferido**: aloja el servicio del destino iSCSI en el sitio preferido.
- **Secundario**: aloja el servicio del destino iSCSI en el sitio secundario.

3 Haga clic en **Aceptar**.

Resultados

El destino iSCSI se crea y se muestra en la sección Destinos iSCSI de vSAN con la información como IQN, el host de propietario de E/S, etc.

Pasos siguientes

Defina la lista de iniciadores iSCSI que podrán acceder a este destino.

Agregar un LUN a un destino iSCSI de vSAN

Puede agregar uno o más LUN a un destino iSCSI de vSAN o editar un LUN existente.

Procedimiento

1 Desplácese hasta el clúster de vSAN.

2 Haga clic en la pestaña **Configurar**.

a En vSAN, haga clic en **Servicio del destino iSCSI**.

b Haga clic en la pestaña Destinos iSCSI y seleccione un destino.

c En la sección de LUN de iSCSI de vSAN, haga clic en **Agregar**. Se abrirá el cuadro de diálogo **Agregar LUN al destino**.

d Introduzca el tamaño del LUN. La directiva de almacenamiento de vSAN configurada para el servicio del destino iSCSI se asignará de forma automática. Puede asignar otra directiva a los LUN.

3 Haga clic en **Agregar**.

Cambiar el tamaño de un LUN en un destino iSCSI de vSAN

En función de sus requisitos, puede aumentar el tamaño de un LUN en línea.

El cambio de tamaño en línea del LUN se habilita solo si todos los hosts del clúster se actualizan a vSAN 6.7 Update 3 o una versión posterior.

Procedimiento

1 En vSphere Client, desplácese hasta el clúster de vSAN.

2 Haga clic en la pestaña **Configurar**.

3 En vSAN, haga clic en **Servicio del destino iSCSI**.

4 Haga clic en la pestaña **Destinos iSCSI** y seleccione un destino.

5 En la sección LUN iSCSI de vSAN, seleccione un LUN y haga clic en **Editar**. Aparece el cuadro de dialogo de Editar LUN.

6 Aumente el tamaño del LUN en función de sus requisitos.

7 Haga clic en **Aceptar**.

Crear un grupo de iniciadores iSCSI de vSAN

Puede crear un grupo de iniciadores iSCSI de vSAN para conceder control de acceso a los destinos iSCSI de vSAN.

Solo los iniciadores iSCSI que sean miembros del grupo de iniciadores podrán acceder a los destinos iSCSI de vSAN.

Nota Los iniciadores fuera del grupo de iniciadores no pueden acceder al destino si el grupo de iniciadores para el control de acceso se creó en el destino iSCSI. Las conexiones actuales de estos iniciadores se perderán y no se podrán recuperar hasta que se agreguen al grupo de iniciadores. Deberá comprobar las conexiones actuales del iniciador y asegurarse de que todos los iniciadores autorizados se agreguen al grupo de iniciadores antes de crear el grupo.

Procedimiento

1 Desplácese hasta el clúster de vSAN.

2 Haga clic en la pestaña **Configurar**.

   a En vSAN, haga clic en **Servicio del destino iSCSI**.

   b Haga clic en la pestaña Grupos de iniciadores y, después, en **Agregar**. Aparecerá el cuadro de diálogo **Nuevo grupo de iniciadores**.

c Escriba un nombre para el grupo de iniciadores iSCSI.

d (Opcional) Para agregar miembros al grupo de iniciadores, escriba el IQN de cada miembro. Use el siguiente formato para introducir el IQN de los miembros:

iqn.YYYY-MM.domain:name

Donde:

- YYYY = año, como 2016
- MM = mes, como 09
- domain = dominio donde se encuentra el iniciador
- name = nombre del miembro (opcional)

3 Haga clic en **Aceptar** o **Crear**.

Pasos siguientes

Agregue miembros al grupo de iniciadores iSCSI.

Asignar un destino a un grupo de iniciadores iSCSI de vSAN

Puede asignar un destino iSCSI a un grupo de iniciadores iSCSI de vSAN.

Solo los iniciadores que sean miembros del grupo de iniciadores podrán acceder a los destinos asignados.

Requisitos previos

Compruebe que haya un grupo de iniciadores iSCSI.

Procedimiento

1 Desplácese hasta el clúster de vSAN.

2 Haga clic en la pestaña **Configurar**.

a En vSAN, haga clic en **Servicio del destino iSCSI**.

b Seleccione la pestaña **Grupos de iniciadores**.

c En la sección Destinos accesibles, haga clic en **Agregar**. Se mostrará el cuadro de diálogo **Agregar destinos accesibles**.

d Seleccione un destino de la lista de destinos accesibles.

3 Haga clic en **Agregar**.

Desactivar el servicio del destino iSCSI de vSAN

Puede desactivar el servicio del destino iSCSI de vSAN.

Al desactivar el servicio del destino iSCSI de vSAN no se eliminan los LUN ni los destinos. Si desea recuperar el espacio, elimine manualmente los LUN o los destinos antes de desactivar el servicio del destino iSCSI de vSAN.

Requisitos previos

Las cargas de trabajo que se ejecutan en los LUN de iSCSI se detienen cuando se desactiva el servicio del destino iSCSI. Antes de desactivarlo, asegúrese de que no haya cargas de trabajo en ejecución en los LUN de iSCSI.

Procedimiento

1 Desplácese hasta el clúster de vSAN y haga clic en **Configurar** > **vSAN** > **Servicios**.

2 En el servicio del destino iSCSI de vSAN, haga clic **EDITAR**.

Se abrirá el asistente Editar el servicio del destino iSCSI de vSAN.

3 Haga clic en el control deslizante **Habilitar el servicio del destino iSCSI de vSAN** para desactivarlo y, a continuación, en **Aplicar**.

Resultados

El servicio del destino iSCSI de vSAN quedará desactivado.

Pasos siguientes

Supervisar el servicio del destino iSCSI de vSAN

Puede supervisar el servicio del destino iSCSI para ver la colocación física de los componentes del destino iSCSI, así como para comprobar los componentes con errores.

También puede supervisar el estado de mantenimiento del servicio del destino iSCSI.

Requisitos previos

Compruebe que se haya habilitado el servicio del destino iSCSI de vSAN y que se hayan creado los destinos y los LUN.

Procedimiento

1 Desplácese hasta el clúster de vSAN.

2 Haga clic en **Supervisar** y, a continuación, seleccione **Objetos virtuales**. Los destinos iSCSI se especifican en la página.

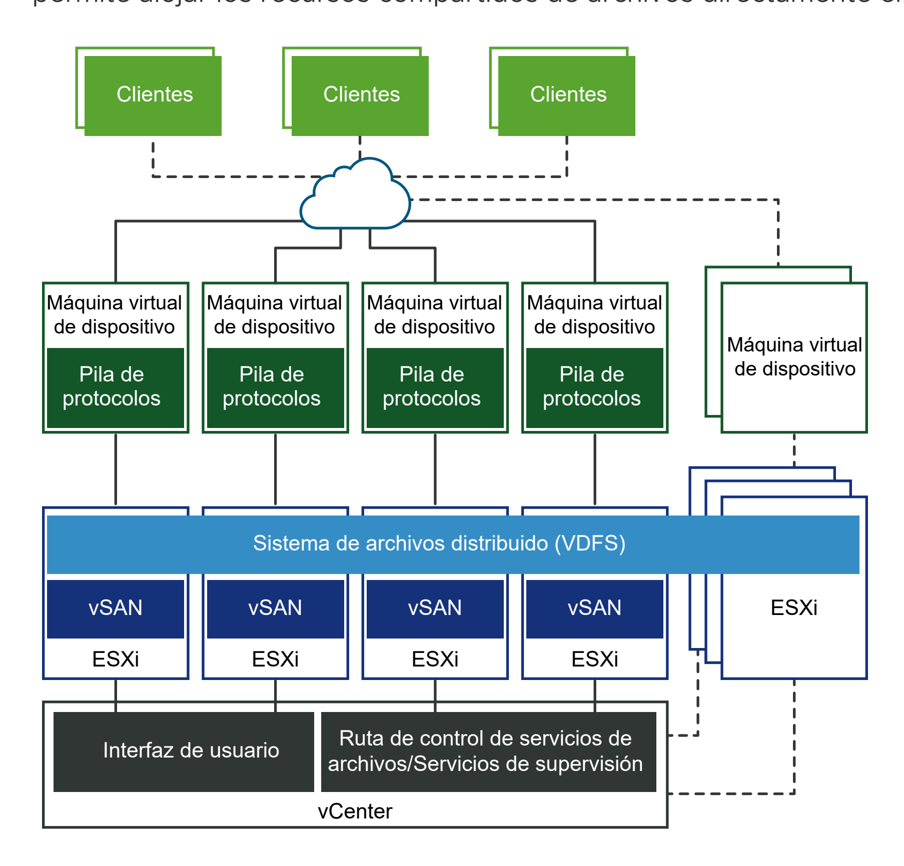
3 Seleccione un destino y haga clic en **Ver los detalles de colocación**. La colocación física muestra el lugar donde se encuentran los componentes de datos del destino.

4 Haga clic en **Componentes del grupo por colocación del host** para ver los hosts asociados con los componentes de datos iSCSI.

Servicio de archivos de vSAN

Utilice el servicio de archivos de vSAN para crear recursos compartidos de archivos en el almacén de datos de vSAN al que pueden acceder las máquinas virtuales o las estaciones de trabajo cliente.

Se puede acceder a los datos almacenados en un recurso compartido de archivos desde cualquier dispositivo que tenga derechos de acceso. El servicio de archivos de vSAN es una capa situada en la parte superior de vSAN que proporciona recursos compartidos de archivos. Actualmente admite recursos compartidos de archivos SMB, NFS 3 y NFS 4.1. El servicio de archivos de vSAN está compuesto por el sistema distribuido de archivos de vSAN (vDFS), que proporciona el sistema de archivos escalable subyacente agregando objetos de vSAN, una plataforma de servicios de almacenamiento que proporciona endpoints de servidores de archivos resistentes y un plano de control para implementación. administración y supervisión. Los recursos compartidos de archivos se integran en la administración de almacenamiento basada en directivas de vSAN existente, y también por uso compartido. El servicio de archivos de vSAN permite alojar los recursos compartidos de archivos directamente en el clúster de vSAN.



Cuando se configura el servicio de archivos de vSAN, vSAN crea un único sistema distribuido de archivos (VDFS) para el clúster que se utilizará internamente con fines de administración. Se coloca una máquina virtual de servicio de archivos (FSVM) en cada host. Las FSVM administran los recursos compartidos de archivos en el almacén de datos de vSAN. Cada FSVM contiene un servidor de archivos que proporciona el servicio NFS y SMB.

Se debe proporcionar un grupo de direcciones IP estáticas como entrada al habilitar el flujo de trabajo del servicio de archivos. Una de las direcciones IP está diseñada como la dirección IP principal. La dirección IP principal se puede utilizar para acceder a todos los recursos compartidos en el clúster de servicios de archivos con la ayuda de las referencias de SMB y NFS 4.1. Para cada dirección IP proporcionada en el grupo de direcciones IP, se inicia un servidor de archivos. Los recursos compartidos de archivos se exportan mediante un único servidor NFS.

Sin embargo, los recursos compartidos de archivos se distribuyen uniformemente entre todos los servidores de archivos. Para proporcionar recursos informáticos que ayuden a administrar las solicitudes de acceso, el número de direcciones IP debe ser igual al número de hosts en el clúster de vSAN.

El servicio de archivos de vSAN admite clústeres ampliados de vSAN y clústeres de vSAN de dos nodos. Un clúster de vSAN de dos nodos debe tener dos servidores de nodos de datos en la misma ubicación u oficina, y el testigo en una ubicación remota o compartida.

Para obtener más información sobre los volúmenes de archivos de almacenamiento nativo en la nube (Cloud Native Storage, CNS), consulte los documentos *VMware vSphere Container Storage Plug-in* y *Configuración y administración de vSphere with Tanzu*.

Limitaciones y consideraciones del servicio de archivos de vSAN

Tenga en cuenta lo siguiente al configurar el servicio de archivos de vSAN:

- vSAN 8.0 admite configuraciones de dos nodos y clústeres ampliados.
- vSAN 8.0 admite 64 servidores de archivos en una configuración de 64 hosts.
- vSAN 8.0 admite 100 recursos compartidos de archivos.
- vSAN 8.0 Update 2 admite el servicio de archivos en Express Storage Architecture (ESA).
- El clúster de vSAN 8.0 Update 3 ESA admite 250 recursos compartidos de archivos. De esos 250 recursos compartidos de archivos, solo un máximo de 100 pueden ser SMB. Por ejemplo, si crea 100 recursos compartidos de archivos SMB, el clúster solo podrá admitir 150 recursos compartidos de archivos NFS adicionales.
- Los servicios de archivos de vSAN no admiten lo siguiente:
  - Controladores de dominio de solo lectura (RODC) para unir dominios, ya que RODC no puede crear cuentas de máquina. Como práctica recomendada de seguridad, se debe crear una unidad organizativa dedicada previamente en Active Directory y el nombre de usuario mencionado aquí debe controlar esta organización.
  - Espacio de nombres independiente.
  - Entornos con varios dominios y un solo bosque de Active Directory.
- Cuando un host entra en modo de mantenimiento, el servidor de archivos se mueve a otra FSVM. Se apagarán las FSVM del host que entró en modo de mantenimiento. Una vez que el host sale del modo de mantenimiento, se encenderá la FSVM.
- La red interna de docker de la máquina virtual de servicios de archivos (FSVM) de vSAN puede superponerse a la red del cliente sin ninguna advertencia ni reconfiguración.

  Se produce un problema de conflicto conocido si la red de servicio de archivos especificada se superpone a la red interna de docker (172.17.0.0/16). Esto provoca un problema de enrutamiento para el tráfico hacia el endpoint correcto.

  Como solución alternativa, especifique una red de servicio de archivos diferente para que no se superponga a la red interna de docker (172.17.0.0/16).

Habilitar el servicio de archivos de vSAN

Puede habilitar los servicios de archivos de vSAN en un clúster de vSAN Original Storage Architecture (OSA) o un clúster de vSAN Express Storage Architecture (ESA).

Requisitos previos

Asegúrese de que esté configurado lo siguiente antes de habilitar los servicios de archivos de vSAN:

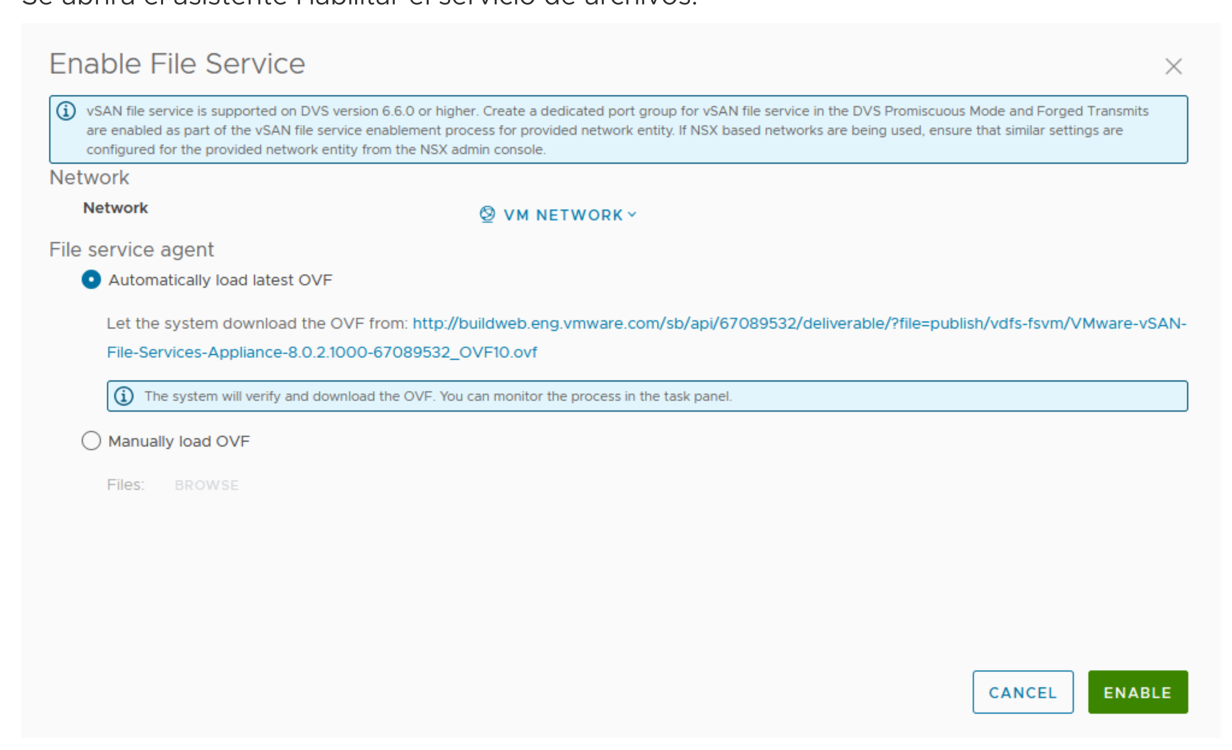
- El clúster de vSAN debe ser un clúster de vSAN normal, un clúster ampliado de vSAN o un clúster ROBO de vSAN.
- Cada host ESXi del clúster vSAN debe tener requisitos de hardware mínimos, como los siguientes:
  - CPU de 4 núcleos
  - Memoria física de 16 GB
- Debe asegurarse de preparar la red como red del servicio de archivos de vSAN:
  - Si usa una red basada en conmutadores estándar, el modo promiscuo y las transmisiones falsificadas se habilitarán como parte del proceso de habilitación de los servicios de archivos de vSAN.
  - Si utiliza una red basada en DVS, los servicios de archivos de vSAN serán compatibles con DVS 6.6.0 o versiones posteriores. Cree un grupo de puertos dedicado para los servicios de archivos de vSAN en DVS. El aprendizaje de direcciones MAC y las transmisiones falsificadas se habilitarán como parte del proceso de habilitación de los servicios de archivos de vSAN para un grupo de puertos DVS proporcionado.
  - **Importante** Si usa una red basada en NSX, asegúrese de que se haya habilitado el aprendizaje de direcciones MAC para la entidad de red proporcionada desde la consola de administración de NSX, y de que todos los nodos de los servicios de archivos y todos los hosts estén conectados a la red de NSX-T deseada.

Procedimiento

1 Desplácese hasta el clúster de vSAN y haga clic en **Configurar** > **vSAN** > **Servicios**.

2 En la fila Servicio de archivos, haga clic en **Habilitar**.

Se abrirá el asistente Habilitar el servicio de archivos.



3 En el menú desplegable **Seleccionar**, seleccione una red.

4 En el Agente del servicio de archivos, seleccione una de las siguientes opciones para descargar el archivo OVF.

Opción	Descripción
Cargar automáticamente OVF más reciente	Esta opción permite que el sistema busque y descargue el archivo OVF. **Nota** ■ Asegúrese de haber configurado el proxy y el firewall para que vCenter pueda acceder al siguiente sitio web y descargue el archivo JSON adecuado. https://download3.vmware.com/software/VSANOVF/FsOvfMapping.json Para obtener más información sobre cómo configurar las opciones de DNS, dirección IP y proxy de vCenter, consulte *Configuración de vCenter Server Appliance*. ■ **Usar OVF actual**: permite utilizar el OVF que ya está disponible. ■ **Cargar automáticamente OVF más reciente**: permite al sistema buscar y descargar el OVF más reciente.
Cargar OVF manualmente	Esta opción le permite examinar y seleccionar un archivo OVF que ya esté disponible en el sistema local. **Nota** Si selecciona esta opción, debe cargar los siguientes archivos: ■ `VMware-vSAN-File-Services-Appliance-x.x.x.x-x_OVF10.mf` ■ `VMware-vSAN-File-Services-Appliance-x.x.x.x-x-x_OVF10.cert` ■ `VMware-vSAN-File-Services-Appliance-x.x.x.x-x-x-system.vmdk` ■ VMware-vSAN-File-Services-Appliance-x.x.x.x-x-cloud-components.vmdk ■ VMware-vSAN-File-Services-Appliance-x.x.x.x-x-log.vmdk ■ VMware-vSAN-File-Services-Appliance-x.x.x.x-x_OVF10.ovf

5 Haga clic en **Habilitar**.

Resultados

- Se descargará e implementará el archivo OVF.
- Los servicios de archivos de vSAN están habilitados.
- Se coloca una máquina virtual de servicios de archivos (FSVM) en cada host.

Nota Las FSVM se administran mediante los servicios de archivos de vSAN. No realice ninguna operación en las FSVM.

Configurar el servicio de archivos de vSAN

Puede configurar el servicio de archivos, que le permite crear recursos compartidos de archivos en el almacén de datos de vSAN.

Requisitos previos

Compruebe lo siguiente antes de configurar el servicio de archivos de vSAN:

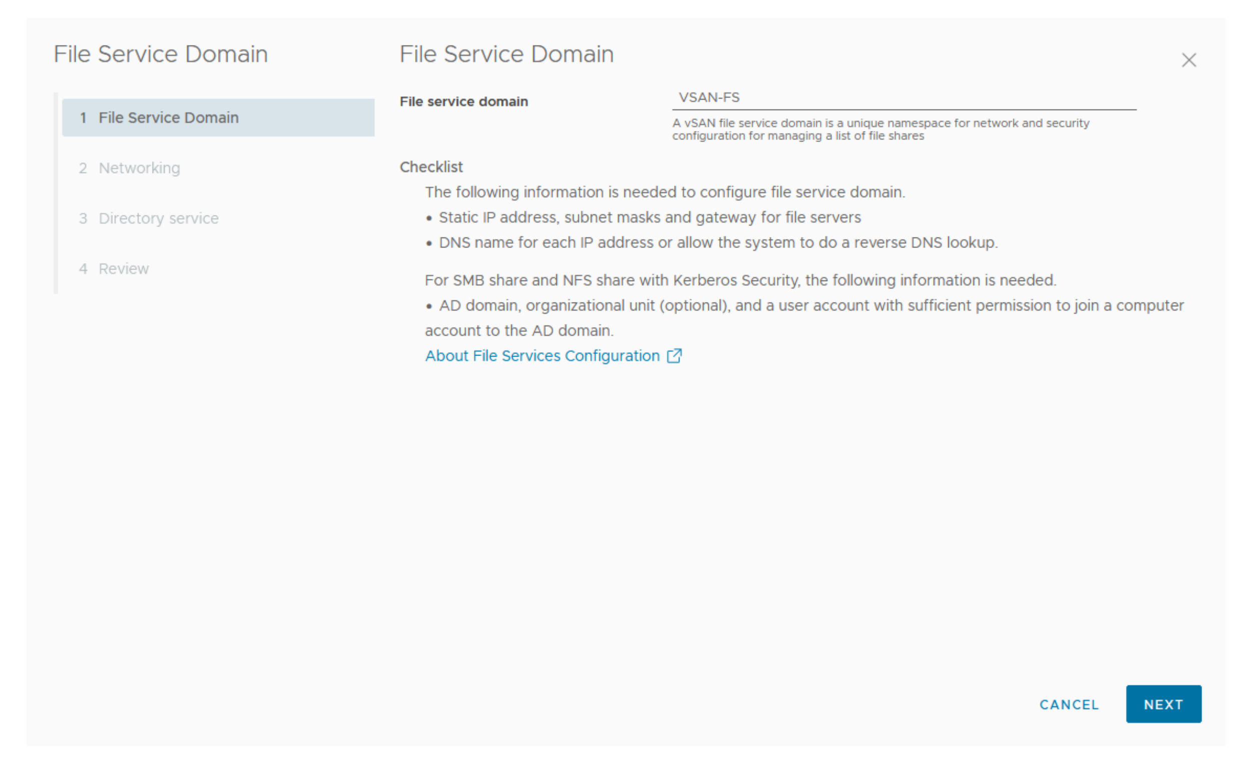
- Habilite el servicio de archivos de vSAN.
- Asigne direcciones IP estáticas como direcciones IP del servidor de archivos desde la red del servicio de archivos de vSAN. Cada IP es el acceso de punto único para los recursos compartidos de archivos de vSAN.
  - Para obtener el mejor rendimiento, el número de direcciones IP debe ser igual al número de hosts en el clúster de vSAN.
  - Todas las direcciones IP estáticas deben ser de la misma subred.
  - Cada dirección IP estáticas tiene un FQDN correspondiente que debe formar parte de las zonas de búsqueda directa e inversa en el servidor DNS.
- Si tiene pensado crear un recurso compartido de archivos SMB basado en Kerberos o un recurso compartido de archivos NFS basado en Kerberos, necesitará lo siguiente:
  - Dominio de Microsoft Active Directory (AD) si proporciona autenticación para crear un recurso compartido de archivos SMB o un recurso compartido de archivos NFS con seguridad de Kerberos.
  - (Opcional) Unidad organizativa de Active Directory para crear todos los objetos del equipo del servidor de archivos.
  - Un usuario de dominio en el servicio de directorio con privilegios suficientes para crear y eliminar objetos de equipo.

Procedimiento

1 Desplácese hasta el clúster de vSAN y haga clic en **Configurar** > **vSAN** > **Servicios**.

2 En la fila Servicio de archivos, haga clic en **Configurar dominio**.

Se abrirá el asistente Dominio del servicio de archivos.



3 En la página Dominio del servicio de archivos, introduzca el espacio de nombres único y haga clic en **Siguiente**. El nombre de dominio debe tener un mínimo de dos caracteres. El primer carácter debe ser un alfabeto o un número. Los caracteres restantes pueden ser un carácter alfabético, un número, un carácter de subrayado (_), un punto (.) o un guion (-).

4 En la página Redes, introduzca la siguiente información y haga clic en **Siguiente**:

- **Protocolo**: puede seleccionar IPv4 o IPv6. El servicio de archivos de vSAN solo admite la pila de IPv4 o IPv6. No se admite la reconfiguración entre IPv4 e IPv6.
- **Servidores DNS**: debe introducir un servidor DNS válido para garantizar la correcta configuración del servicio de archivos.
- **Sufijos DNS**: proporcione el sufijo DNS que se utiliza con el servicio de archivos. También se deben incluir los demás sufijos DNS desde los que los clientes puedan acceder a estos servidores de archivos. El servicio de archivos no admiten el dominio DNS con una sola etiqueta, como "app", "wiz", "com", etc. Un nombre de dominio asignado al servicio de archivos debe tener el formato estedominio.nombrednsraízregistrado. El nombre de DNS y el sufijo deben cumplir las prácticas recomendadas que se detallan en https://docs.microsoft.com/es-es/windows-server/identity/ad-ds/plan/selecting-the-forest-root-domain.
- **Máscara de subred**: introduzca una máscara de subred válida. Este cuadro de texto aparece al seleccionar IPv4.

- **Longitud de prefijo**: introduzca un número entre 1 y 128. Este cuadro de texto aparece al seleccionar IPv6.
- **Puerta de enlace**: introduzca una puerta de enlace válida.
- **Grupo de direcciones IP**: introduzca la dirección IP principal y el nombre de DNS.

Con vSAN 8.0 Update 3, el clúster de vSAN ESA admite 250 recursos compartidos de archivos. De esos 250 recursos compartidos de archivos, solo un máximo de 100 pueden ser SMB. Por ejemplo, si crea 100 recursos compartidos de archivos SMB, el clúster solo podrá admitir 150 recursos compartidos de archivos NFS adicionales.

Cada servidor de archivos de un clúster de vSAN ESA puede admitir un máximo de 25 recursos compartidos de archivos y requiere que al menos 10 direcciones IP tengan el máximo de 250 recursos compartidos. Con el aumento de los servidores de archivos o los recursos compartidos de archivos por host, es posible que el rendimiento del servicio de archivos de vSAN se vea afectado. Para obtener el mejor rendimiento, el número de direcciones IP debe ser igual al número de hosts en el clúster de vSAN.

La opción Sitio de afinidad está disponible si va a configurar el servicio de archivos de vSAN en un clúster ampliado de vSAN. Esta opción permite configurar la colocación del servidor de archivos en el sitio **Preferido** o **Secundario**. Esto ayuda a reducir la latencia de tráfico entre sitios. El valor predeterminado es **Cualquiera**, lo que indica que no se aplica ninguna regla de afinidad del sitio al servidor de archivos.

Nota Si el clúster es un clúster ROBO, asegúrese de que el valor del sitio de afinidad esté establecido en **Cualquiera**.

En un evento de error de sitio, el servidor de archivos asociado a ese sitio conmuta por error al otro sitio. El servidor de archivos vuelve al sitio afiliado cuando se recupera. Configure más servidores de archivos en un sitio si se esperan más cargas de trabajo de un sitio determinado.

Nota Si el servidor de archivos contiene recursos compartidos de archivos SMB, no se realizará una conmutación por recuperación automáticamente aunque se recupere el error del sitio.

Tenga en cuenta lo siguiente al configurar las direcciones IP y los nombres DNS:

- Para garantizar la correcta configuración del servicio de archivos, las direcciones IP que introduzca en la página Redes deben ser direcciones estáticas, y el servidor DNS debe tener registros para dichas direcciones IP. Para obtener el mejor rendimiento, el número de direcciones IP debe ser igual al número de hosts en el clúster de vSAN.
- Puede tener un máximo de 64 hosts en el clúster. Si se configura la compatibilidad con clústeres de gran escala, puede introducir hasta 64 direcciones IP.
- Puede usar las siguientes opciones para rellenar automáticamente los cuadros de texto Dirección IP y Nombre del servidor DNS:

AUTORELLENAR: esta opción se muestra después de introducir la primera dirección IP en el cuadro de texto Dirección IP. Haga clic en la opción AUTORELLENAR para rellenar automáticamente el resto de campos con direcciones IP secuenciales, en función de la máscara de subred y la dirección de la puerta de enlace de la dirección IP que haya introducido en la primera fila. Puede editar las direcciones IP rellenadas automáticamente.

BÚSQUEDA DE DNS: esta opción se muestra después de introducir la primera dirección IP en el cuadro de texto Dirección IP. Haga clic en la opción BÚSQUEDA DE DNS para recuperar automáticamente el FQDN correspondiente a las direcciones IP en la columna Dirección IP.

Nota

- Todas las reglas válidas se aplican a los FQDN. Para obtener más información, consulte https://tools.ietf.org/html/rfc953.
- La primera parte del FQDN, también conocida como Nombre de NetBIOS, no debe tener más de 15 caracteres.

Los FQDN se recuperan automáticamente solo en las siguientes condiciones:

- Debe haber introducido un servidor DNS válido en la página Dominio.
- Las direcciones IP introducidas en la página Grupo de direcciones IP deben ser direcciones estáticas, y el servidor DNS debe tener registros para dichas direcciones IP.

5 En la página Servicio de directorio, introduzca la siguiente información y haga clic en **Siguiente**.

Opción	Descripción
Servicio de directorio	Configure un dominio de Active Directory en el servicio de archivos de vSAN para la autenticación. Si desea crear un recurso compartido de archivos SMB o un recurso compartido de archivos NFS 4.1 con autenticación Kerberos, debe configurar un dominio de AD para el servicio de archivos de vSAN.
Dominio de AD	Nombre de dominio completo al que se ha unido el servidor de archivos.
Servidor AD preferido	Introduzca la dirección IP del servidor de AD preferido. Si introduce varias direcciones IP, asegúrese de que estén separadas por comas.

Opción	Descripción
Unidad organizativa (opcional)	Contiene la cuenta de equipo que crea el servicio de archivos de vSAN. En una organización con jerarquías complejas, cree la cuenta de equipo en un contenedor determinado usando una barra diagonal para indicar las jerarquías (por ejemplo, unidad_organizativa/unidad_organizativa_interna). **Nota** De forma predeterminada, el servicio de archivos de vSAN crea la cuenta de equipo en el contenedor de equipos.
Nombre de usuario de AD	Nombre de usuario que se utilizará para conectar y configurar el servicio de Active Directory. Este nombre de usuario autentica Active Directory en el dominio. Un usuario de dominio autentica el controlador de dominio y crea las cuentas de equipo del servicio de archivos de vSAN, las entradas de SPN relacionadas y las entradas de DNS de archivos (cuando se utiliza Microsoft DNS). Como práctica recomendada, cree una cuenta de servicio dedicada para el servicio de archivos. Un usuario de dominio en el servicio de directorio con los siguientes privilegios para crear y eliminar objetos de equipo: ■ (Opcional) Agregar/actualizar entradas de DNS
Contraseña	Contraseña del nombre de usuario de Active Directory en el dominio. El servicio de archivos de vSAN utilizan la contraseña para autenticarse en AD y para crear la cuenta de equipo del servicio de archivos de vSAN.

Nota

- El servicio de archivos de vSAN no admite lo siguiente:
  - Controladores de dominio de solo lectura (RODC) para unir dominios, ya que RODC no puede crear cuentas de máquina. Como práctica recomendada de seguridad, se debe crear una unidad organizativa dedicada previamente en Active Directory, y el nombre de usuario mencionado aquí debe controlar esta organización.
  - Espacio de nombres independiente.
  - Entornos con varios dominios y un solo bosque de Active Directory.
- Solo se admiten caracteres del alfabeto inglés para el nombre de usuario de Active Directory.
- Solo se admite una configuración de dominio de AD único. Sin embargo, los servidores de archivos se pueden poner en un subdominio DNS válido. Por ejemplo, un dominio de AD con el nombre `example.com` puede tener el FQDN de servidor de archivos como `name1.eng.example.com`.
- No se admiten los objetos de equipo creados previamente para servidores de archivos. Asegúrese de que el usuario proporcionado aquí tenga privilegios suficientes en la unidad organizativa.
- El servicio de archivos de vSAN actualiza los registros de DNS de los servidores de archivos si Active Directory también se utiliza como servidor DNS y el usuario tiene permisos suficientes para actualizar los registros de DNS. El servicio de archivos de vSAN también tiene una comprobación de estado que indica si las búsquedas directas e inversas de los servidores de archivos funcionan correctamente. Sin embargo, si hay otras soluciones de propiedad que se utilizan como servidores DNS, el administrador de Vi debe actualizar estos registros de DNS.

---

6 Revise la configuración y haga clic en **Finalizar**.

Resultados

El dominio del servicio de archivos está configurado. Los servidores de archivos se inician con las direcciones IP que se asignaron durante el proceso de configuración del servicio de archivos de vSAN.

Editar el servicio de archivos de vSAN

Puede editar y reconfigurar los ajustes de un servicio de archivos de vSAN.

Requisitos previos

- Si va a actualizar de vSAN 7.0 a 7.0 Update 1, puede crear recursos compartidos de archivos Kerberos SMB y NFS. Para ello, es necesario configurar el dominio de Active Directory para el servicio de archivos de vSAN.

- Si hay recursos compartidos activos, no se permite cambiar el dominio de Active Directory, ya que esta acción puede interrumpir los permisos de usuario en los recursos compartidos activos.
- Si se cambió la contraseña de Active Directory, puede editar las opciones de configuración de Active Directory y proporcionar la nueva contraseña.

Nota Esta acción puede provocar una interrupción mínima en las operaciones de E/S de Inflight en los recursos compartidos de archivos.

Procedimiento

1 Desplácese hasta el clúster de vSAN y haga clic en **Configurar** > **vSAN** > **Servicios**.

2 En la fila Servicio de archivos, haga clic en **Editar**> **Editar dominio**.

Se abrirá el asistente Dominio del servicio de archivos.

3 En la página Dominio del servicio de archivos, edite el nombre de dominio del servicio de archivos y haga clic en **Siguiente**.

4 En la página Redes, introduzca la los cambios de configuración necesarios y haga clic en **Siguiente**. Puede editar las direcciones IP principales, las direcciones IP estáticas y los nombres DNS. Puede agregar o eliminar las direcciones IP principales o las direcciones IP estáticas. No puede cambiar el nombre de DNS sin cambiar la IP.

Nota El cambio de la información del dominio es una acción disruptiva. Es posible que requiera a todos los clientes utilizar nuevas URL para volver a conectarse a los recursos compartidos de archivos.

5 En la página del servicio de directorio, realice los cambios pertinentes relacionados con el directorio y haga clic en **Siguiente**.

Nota No podrá cambiar el dominio de AD, la unidad organizativa ni el nombre de usuario una vez que haya configurado los servicios de archivos de vSAN.

6 En la página Revisar, haga clic en **Finalizar** después de realizar los cambios necesarios.

Resultados

Los cambios se aplicarán a la configuración del servicio de archivos de vSAN.

Crear un recurso compartido de archivos de vSAN

Cuando el servicio de archivos de vSAN está habilitado, puede crear uno o varios recursos compartidos de archivos en el almacén de datos de vSAN.

El servicio de archivos de vSAN no admite el uso de recursos compartidos de archivos NFS en ESXi.

Requisitos previos

Si va a crear un recurso compartido de archivos SMB o un recurso compartido de archivos NFS 4.1 con seguridad Kerberos, asegúrese de haber configurado el servicio de archivos de vSAN en un dominio de AD.

Consideraciones sobre el uso y el nombre del recurso compartido

- Se pueden utilizar nombres de usuario con caracteres que no son ASCII para acceder a los datos de los recursos compartidos.
- Los nombres de los recursos compartidos no pueden superar los 80 caracteres y solo pueden contener caracteres en inglés, números y guiones. Todos los guiones deben ir precedidos y seguidos por un número o una letra. No se permiten guiones consecutivos.
- Para los recursos compartidos de tipo SMB, el archivo y los directorios pueden contener cualquier cadena Unicode compatible.
- Para los recursos compartidos de tipo NFS 4 puros, el archivo y los directorios pueden contener cualquier cadena compatible con UTF-8.
- Para los directorios y archivos de recursos compartidos de NFS 3 y NFS 3 + NFS 4, solo puede contener cadenas compatibles con ASCII.
- La migración de datos de recursos compartidos de NFS 3 antiguos a recursos compartidos nuevos del servicio de archivos de vSAN con NFS 4 solo requiere la conversión de todos los nombres de archivos y directorios a la codificación UTF-8. Hay herramientas de terceros para lograr los mismo.

Procedimiento

1 Desplácese hasta el clúster de vSAN y haga clic en **Configurar** > **vSAN** > **Recursos compartidos de archivos**.

   Con vSAN 8.0 Update 3, el clúster de vSAN ESA admite 250 recursos compartidos de archivos. De esos 250 recursos compartidos de archivos, solo un máximo de 100 pueden ser SMB. Por ejemplo, si crea 100 recursos compartidos de archivos SMB, el clúster solo podrá admitir 150 recursos compartidos de archivos NFS adicionales.

   Cada servidor de archivos de un clúster de vSAN ESA puede admitir un máximo de 25 recursos compartidos de archivos y requiere que al menos 10 direcciones IP tengan el máximo de 250 recursos compartidos. Con el aumento de los servidores de archivos o los recursos compartidos de archivos por host, es posible que el rendimiento del servicio de archivos de vSAN se vea afectado. Para obtener el mejor rendimiento, el número de direcciones IP debe ser igual al número de hosts en el clúster de vSAN.

2 Haga clic en **Agregar**.

   Se abrirá el asistente Crear recurso compartido de archivos.

3 En la página General, introduzca la siguiente información y haga clic en **Siguiente**.

   - **Nombre**: introduzca un nombre para el archivo.

- **Protocolo**: seleccione un protocolo adecuado. El servicio de archivos de vSAN admite los protocolos de sistema de archivos SMB y NFS.

  Si selecciona el protocolo **SMB**, también puede configurar el recurso compartido de archivos SMB para que acepte únicamente los datos cifrados mediante la opción **Cifrado de protocolo**.

  Si selecciona el protocolo **NFS**, puede configurar el recurso compartido de archivos para que admita **NFS 3**, **NFS 4** o ambas versiones (**NFS 3 y NFS 4**). Si selecciona la versión **NFS 4**, puede establecer **AUTH_SYS** o la seguridad **Kerberos**.

  Nota El protocolo SMB y la seguridad Kerberos para el protocolo NFS solo pueden configurarse si el servicio de archivos de vSAN está configurado con Active Directory. Para obtener más información, consulte Configurar el servicio de archivos de vSAN.

- Con el protocolo SMB, puede ocultar las carpetas y los archivos para los que el usuario cliente compartido no tiene permiso de acceso mediante la opción **Enumeración basada en acceso**.
- **Directiva de almacenamiento**: seleccione una directiva de almacenamiento adecuada.
- **Sitio de afinidad**: esta opción está disponible si va a crear un recurso compartido de archivos en un clúster ampliado de vSAN. Esta opción le ayuda a colocar el recurso compartido de archivos en un servidor de archivos que pertenece al sitio que elija. Utilice esta opción cuando prefiera una latencia baja al acceder al recurso compartido de archivos. El valor predeterminado es **Cualquiera**, lo que indica que el recurso compartido de archivos se coloca en un sitio con menos tráfico preferido o secundario.
- **Cuotas de espacio de almacenamiento**: puede establecer los siguientes valores:
  - **Umbral de advertencia de recurso compartido**: cuando el recurso compartido alcanza este umbral, se muestra un mensaje de advertencia.
  - **Cuota máxima de recurso compartido**: cuando el recurso compartido alcanza este umbral, se deniega la nueva asignación de bloques.
- **Etiquetas**: una etiqueta es un par clave-valor que le ayuda a organizar los recursos compartidos de archivos. Puede asignar etiquetas a los recursos compartidos de archivos y, a continuación, filtrarlos por etiquetas. La clave de una etiqueta es una cadena con 1~250 caracteres. El valor de una etiqueta es una cadena cuya longitud debe ser inferior a 1000 caracteres. El servicio de archivos de vSAN admite hasta 5 etiquetas por recurso compartido.

4 La página Control de acceso de red incluye opciones para definir el acceso al recurso compartido de archivos. Las opciones de control de acceso de red solo están disponibles para los recursos compartidos de NFS. Seleccione una de las siguientes opciones y haga clic en **Siguiente**.

- **Sin acceso**: seleccione esta opción para que no se pueda acceder al recurso compartido de archivos desde cualquier dirección IP.

- **Permitir acceso desde cualquier IP**: seleccione esta opción para que el recurso compartido de archivos sea accesible desde todas las direcciones IP.
- **Personalizar el acceso a la red**: seleccione esta opción para definir los permisos de direcciones IP específicas. Con esta opción, puede especificar si una dirección IP concreta puede acceder, realizar cambios o solo leer el recurso compartido de archivos. También puede habilitar **Denegación de raíz** en cada dirección IP. Puede escribir las direcciones IP con los formatos siguientes:
  - Una sola dirección IP. Por ejemplo, 123.23.23.123
  - Dirección IP junto con una máscara de subred. Por ejemplo, 123.23.23.0/8
  - Un rango, especificando una dirección IP de inicio y una dirección IP de finalización separadas por un guion (-). Por ejemplo, 123.23.23.123-123.23.23.128
  - Asterisco (*) para implicar a todos los clientes.

5. En la página Revisar, revise la configuración y, a continuación, haga clic en **Finalizar**.

   Se crea un nuevo recurso compartido de archivos en el almacén de datos de vSAN.

Ver recursos compartidos de archivos de vSAN

Puede ver la lista de recursos compartidos de archivos de vSAN.

Para ver la lista de recursos compartidos de archivos de vSAN, desplácese hasta el clúster de vSAN y haga clic en **Configurar** > **vSAN** > **Recursos compartidos del servicio de archivos**.

Se mostrará una lista de los recursos compartidos de archivos de vSAN. Para cada recurso compartido de archivos, puede ver información como la directiva de almacenamiento, la cuota máxima, el uso que sobrepasa la cuota, el uso real, etc. El clúster de vSAN ESA muestra el número de recursos compartidos de archivos existentes y el límite máximo de recursos compartidos de archivos permitido en un clúster.

Acceder a recursos compartidos de archivos de vSAN

Puede acceder a un recurso compartido de archivos desde un cliente de host.

Acceder a un recurso compartido de archivos NFS

Puede acceder a un recurso compartido de archivos desde un cliente de host mediante un sistema operativo que se comunica con los sistemas de archivos NFS. En el caso de las distribuciones de Linux basadas en RHEL, la compatibilidad de NFS 4.1 está disponible en RHEL 7.3 y en la CentOS 7.3-1611 en un kernel 3.10.0-514 o posterior. Para las distribuciones de Linux basadas en Debian, la compatibilidad de NFS 4.1 está disponible en Linux kernel 4.0.0 o versiones posteriores. Todos los clientes NFS deben tener nombres de host únicos para que NFS 4.1 funcione. Puede usar el comando mount de Linux con la IP principal para montar un recurso compartido de archivos de vSAN en el cliente. Por ejemplo: `mount -t nfs4 -o minorversion=1,sec=sys <primary ip>:/vsanfs/<share name>`. NFS 3 es compatible con distribuciones de Linux basadas en RHEL y Debian. Puede usar el comando mount de Linux para

montar un recurso compartido de archivos de vSAN en el cliente. Por ejemplo: mount `-t nfs vers=3 <nfsv3_access_point> <localmount_point>`.

Ejemplo

Ejemplos de comandos v41 para verificar el recurso compartido de archivos de NFS desde un cliente de host:

```
[root@localhost ~]# mount -t nfs4 -o minorversion=1,sec=sys <primary ip address>:/vsanfs/
TestShare-0 /mnt/TestShare-0
[root@localhost ~]# cd /mnt/TestShare-0/
[root@localhost TestShare-0]# mkdir bar
[root@localhost TestShare-0]# touch foo
[root@localhost TestShare-0]# ls -l
total 0
drwxr-xr-x. 1 root root 0 Feb 19 18:35 bar
-rw-r--r--. 1 root root 0 Feb 19 18:35 foo
```

Acceder al recurso compartido de archivos de Kerberos NFS

Un cliente Linux que accede a un recurso compartido de Kerberos NFS debe tener un ticket de Kerberos válido.

Ejemplos de comandos v41 para verificar el recurso compartido de archivos de Kerberos NFS desde un cliente de host:

Se puede montar un recurso compartido de Kerberos NFS mediante el siguiente comando de montaje:

```
[root@localhost ~]# mount -t nfs4 -o minorversion=1,sec=krb5/krb5i/krb5p <primary ip
address>:/vsanfs/TestShare-0 /mnt/TestShare-0
[root@localhost ~]# cd /mnt/TestShare-0/
[root@localhost TestShare-0]# mkdir bar
[root@localhost TestShare-0]# touch foo
[root@localhost TestShare-0]# ls -l
total 0
drwxr-xr-x. 1 root root 0 Feb 19 18:35 bar
-rw-r--r--. 1 root root 0 Feb 19 18:35 foo
```

Cambiar la propiedad de un recurso compartido de Kerberos NFS

Debe iniciar sesión con el nombre de usuario del dominio de AD para cambiar la propiedad de un recurso compartido. El nombre de usuario del dominio de AD proporcionado en la configuración del servicio de archivos actúa como un usuario sudo para el recurso compartido de archivos de Kerberos.

```
[root@localhost ~]# mount -t nfs4 -o minorversion=1,sec=sys <primary ip address>:/vsanfs/
TestShare-0 /mnt/TestShare-0
[fsadmin@ocalhost ~]# chown user1 /mnt/TestShare-0
[user1@localhost ~]# ls -l /mnt/TestShare-0
total 0
```

```
drwxr-xr-x. 1 user1 domain  users 0 Feb 19 18:35 bar
-rw-r--r--. 1 user1 domain users 0 Feb 19 18:35 foo
```

Acceder a un recurso compartido de archivos SMB

Puede acceder a un recurso compartido de archivos SMB desde un cliente Windows.

Requisitos previos

Asegúrese de que el cliente Windows esté unido al dominio de Active Directory configurado con el servicio de archivos de vSAN.

Procedimiento

1 Copie la ruta del recurso compartido de archivos SMB mediante el siguiente procedimiento:

   a Desplácese hasta el clúster de vSAN y haga clic en **Configurar** > **vSAN** > **Recursos compartidos del servicio de archivos**.

      Se mostrará una lista de todos los recursos compartidos de archivos de vSAN.

   b Seleccione el recurso compartido de archivos SMB al que desea acceder desde el cliente Windows.

   c Haga clic en **COPIAR RUTA** > **SMB**.

      La ruta del recurso compartido de archivos SMB se copiará en el portapapeles.

2 Inicie sesión en el cliente Windows como un usuario de dominio de Active Directory normal.

3 Acceda al recurso compartido de archivos SMB usando la ruta de acceso que ha copiado.

Editar un recurso compartido de archivos de vSAN

Puede editar la configuración de un recurso compartido de archivos de vSAN.

Procedimiento

1 Desplácese hasta el clúster de vSAN y haga clic en **Configurar** > **vSAN** > **Recursos compartidos del servicio de archivos**.

   Se mostrará una lista de todos los recursos compartidos de archivos de vSAN.

2 Seleccione el recurso compartido de archivos que desea modificar y haga clic en **EDITAR**.

3 En la página Editar recurso compartido de archivos, realice los cambios necesarios en la configuración del recurso compartido de archivos y haga clic en **Finalizar**.

Resultados

La configuración del recurso compartido de archivos se actualizará.

Nota vSAN no permite el cambio de protocolo de recurso compartido de archivos entre SMB y NFS.

Administrar un recurso compartido de archivos SMB en un clúster de vSAN

El servicio de archivos de vSAN admite el complemento Carpetas compartidas de Microsoft Management Console (MMC) para administrar los recursos compartidos de SMB en el clúster de vSAN.

Puede realizar las siguientes tareas en recursos compartidos de SMB del sistema de archivos de vSAN usando la herramienta MMC:

- Administrar la lista de control de acceso (ACL).
- Cerrar archivos abiertos.
- Ver sesiones activas.
- Ver archivos abiertos.
- Cerrar conexiones de clientes.

Procedimiento

1. Copie el comando de MMC mediante el siguiente procedimiento:
   a. Desplácese hasta el clúster de vSAN y haga clic en **Configurar** > **vSAN** > **Recursos compartidos del servicio de archivos**.

      Se mostrará una lista de todos los recursos compartidos de archivos de vSAN.
   b. Seleccione el recurso compartido de archivos SMB que desea administrar desde el cliente Windows mediante la herramienta MMC.
   c. Haga clic en **COPIAR COMANDO DE MMC**.

      El comando de MMC se copiará en el portapapeles.
2. Inicie sesión en el cliente de Windows como usuario administrador del servicio de archivos. El usuario admin del servicio de archivos se configura al crear el dominio del servicio de archivos. Un usuario administrador del servicio de archivos tiene todos los privilegios en el servidor de archivos.
3. En el cuadro de búsqueda de la barra de tareas, escriba Ejecutar y, a continuación, seleccione **Ejecutar**.
4. En el cuadro Ejecutar, ejecute el comando de MMC que ha copiado para acceder y administrar el recurso compartido de SMB mediante la herramienta MMC.

Eliminar un recurso compartido de archivos de vSAN

Puede eliminar un recurso compartido de archivos si ya no lo necesita.

Al eliminar un recurso compartido de archivos, también se eliminan todas las instantáneas asociadas a ese recurso compartido de archivos.

Procedimiento

1 Desplácese hasta el clúster de vSAN y haga clic en **Configurar** > **vSAN** > **Recursos compartidos del servicio de archivos**.

   Se mostrará una lista de todos los recursos compartidos de archivos de vSAN.

2 Seleccione el recurso compartido de archivos que desea modificar y haga clic en **ELIMINAR**.

3 En el cuadro de diálogo Eliminar recursos compartidos de archivos, haga clic en **ELIMINAR**.

Instantánea del sistema de archivos distribuido de vSAN

Una instantánea proporciona un archivo basado en tiempo que aprovecha el espacio de forma eficiente.

Permite recuperar datos de un archivo o un conjunto de archivos en caso de que se eliminen accidentalmente. Una instantánea del sistema de archivos proporciona información sobre los archivos que se cambiaron y los cambios realizados en el archivo. Proporciona un servicio de recuperación de archivos automatizado y es más eficiente en comparación con el método de copia de seguridad tradicional basado en cintas. Un instantánea en sí misma no es una solución de recuperación ante desastres completa, pero los proveedores de copia de seguridad de terceros pueden utilizarla para copiar los archivos modificados (copia de seguridad incremental) en una ubicación física diferente.

Los servicios de archivos de vSAN tienen una función integrada que permite crear una imagen en un momento específico del recurso compartido de archivos de vSAN. Cuando el servicio de archivos de vSAN está habilitado, puede crear hasta 32 instantáneas por recurso compartido. Una instantánea de un recurso compartido de archivos de vSAN es una instantánea del sistema de archivos que proporciona una imagen de un momento específico de un recurso compartido de archivos de vSAN.

Nota La instantánea del sistema de archivos distribuido de vSAN es compatible con la versión 7.0 Update 2 o posteriores.

Consideraciones para las instantáneas del sistema de archivos

- Utilice Predeterminado como nombre de la instantánea para recuperar los datos.
- El nombre de la instantánea no puede tener más de 100 caracteres y solo puede contener caracteres en inglés, números y caracteres especiales, excepto los siguientes:
  - " (ASCII 34)
  - $ (ASCII 36)
  - % (ASCII 37)
  - & (ASCII 38)
  - * (ASCII 42)
  - / (ASCII 47)

- : (ASCII 58)
- < (ASCII 60)
- > (ASCII 62)
- ? (ASCII 63)
- \ (ASCII 92)
- ^ (ASCII 94)
- | (ASCII 124)
- ~ (ASCII 126)

Crear una instantánea

Cuando el servicio de archivos de vSAN está habilitado, se pueden crear una o varias instantáneas que proporcionan una imagen en un momento específico del recurso compartido de archivos de vSAN. Puede crear un máximo de 32 instantáneas por recurso compartido de archivos.

Requisitos previos

Debe haber creado un recurso compartido de archivos de vSAN.

Procedimiento

1. Desplácese hasta el clúster de vSAN y haga clic en **Configurar** > **vSAN** > **Recursos compartidos del servicio de archivos**.

   Se mostrará una lista de los recursos compartidos de archivos de vSAN.

2. Seleccione el recurso compartido de archivos para el que desea crear una instantánea y, a continuación, haga clic en **INSTANTÁNEAS** > **NUEVA INSTANTÁNEA**.

   Aparecerá el cuadro de diálogo Crear nueva instantánea.

3. En el cuadro de diálogo Crear nueva instantánea, proporcione un nombre para la instantánea y haga clic en **Crear**.

Resultados

Se creará una instantánea de un momento específico para el recurso compartido de archivos seleccionado.

Ver una instantánea

Puede ver la lista de instantáneas junto con información como la fecha y hora de creación y el tamaño.

Procedimiento

1 Desplácese hasta el clúster de vSAN y haga clic en **Configurar** > **vSAN** > **Recursos compartidos del servicio de archivos**.

Se mostrará una lista de los recursos compartidos de archivos de vSAN.

2 Seleccione un recurso compartido de archivos y haga clic en **INSTANTÁNEAS**.

Resultados

Aparecerá una lista de instantáneas de ese recurso compartido de archivos. Podrá ver información como la fecha y hora de creación de la instantánea y su tamaño.

Eliminar una instantánea

Puede eliminar una instantánea si ya no la necesita.

Procedimiento

1 Desplácese hasta el clúster de vSAN y haga clic en **Configurar** > **vSAN** > **Recursos compartidos del servicio de archivos**.

Se mostrará una lista de los recursos compartidos de archivos de vSAN.

2 Seleccione un recurso compartido de archivos y haga clic en **INSTANTÁNEAS**.

Aparecerá una lista de instantáneas pertenecientes al recurso compartido de archivos seleccionado.

3 Seleccione la instantánea que desee eliminar y, a continuación, haga clic en **ELIMINAR**.

Volver a equilibrar la carga de trabajo en hosts del servicio de archivos de vSAN

Skyline Health muestra el estado de mantenimiento del equilibrio de carga de trabajo para todos los hosts que forman parte de la infraestructura del servicio de archivos de vSAN.

Si hay un desequilibrio en la carga de trabajo de un host, puede corregirlo reequilibrando la carga de trabajo.

Requisitos previos

Procedimiento

1 Desplácese hasta el clúster de vSAN y, a continuación, haga clic en **Supervisar** > **vSAN** > **Skyline Health**.

2 En Skyline Health, expanda **Servicio de archivos** y, a continuación, haga clic en **Estado de la infraestructura**.

   La pestaña Estado de la infraestructura mostrará una lista de todos los hosts que forman parte de la infraestructura del servicio de archivos de vSAN. Para cada host, se mostrará el estado del equilibrio de la carga de trabajo. Si hay un desequilibrio en la carga de trabajo de un host, se mostrará una alerta en la columna **Descripción**.

3 Haga clic en **CORREGIR DESEQUILIBRIO** y, a continuación, **REDISTRIBUCIÓN** para corregir el desequilibrio.

   Antes de continuar con el reequilibrado, tenga en cuenta lo siguiente:

   - Durante el reequilibrado de la carga, es posible que los contenedores de los hosts con una carga de trabajo desequilibrada se muevan a otros hosts. La actividad de reequilibrado también puede afectar a los otros hosts del clúster.
   - Durante el proceso de reequilibrado, las cargas de trabajo que se ejecutan en recursos compartidos de NFS no se interrumpen. Sin embargo, las E/S a los recursos compartidos de SMB ubicados en los contenedores que se movieron se interrumpirán.

Resultados

La carga de trabajo del host se equilibrará y el estado de equilibrio de la carga de trabajo se mostrará en verde.

Recuperar espacio con anulación de asignación en el sistema de archivos distribuidos de vSAN

Los comandos UNMAP permiten recuperar espacio de almacenamiento que se asigna a archivos eliminados en el sistema de archivos distribuidos de vSAN (VDFS) creado por el invitado en el objeto de vSAN.

vSAN 6.7 Update 2 y versiones posteriores admiten los comandos UNMAP. Al eliminar o quitar los archivos y las instantáneas, se libera espacio en el sistema de archivos. Este espacio libre queda asignado a un dispositivo de almacenamiento hasta que el sistema de archivos lo libera o anula la asignación. vSAN admite la recuperación de espacio libre, también denominada operación de anulación de asignación. Puede liberar espacio de almacenamiento en el VDFS cuando se eliminan los recursos compartidos de archivos y las instantáneas, cuando se consolidan los recursos compartidos de archivos y las instantáneas, etc. Puede anular la asignación del espacio de almacenamiento al eliminar archivos o instantáneas.

La capacidad de anulación de asignación no está habilitada de forma predeterminada. Para habilitar la anulación de asignación en un clúster de vSAN, utilice el siguiente comando de RVC:

```
vsan.unmap_support –enable
```

Cuando habilite la anulación de asignación en un clúster de vSAN, deberá apagar y volver a encender todas las máquinas virtuales. Las máquinas virtuales deben usar hardware virtual versión 13 o posterior para poder realizar operaciones de anulación de asignación.

Actualizar el servicio de archivos de vSAN

Cuando se actualiza el servicio de archivos, la actualización se realiza de forma gradual.

Durante la actualización, los contenedores de servidores de archivos que se ejecutan en las máquinas virtuales que se están actualizando se conmutan por error a otras máquinas virtuales. Los recursos compartidos de archivos seguirán accesibles durante la actualización. Durante la actualización, es posible que se produzcan algunas interrupciones al acceder a los recursos compartidos de archivos.

Requisitos previos

Asegúrese de que se hayan actualizado los siguientes elementos:

- Hosts ESXi
- vCenter Server
- formato de disco de vSAN

Procedimiento

1 Desplácese hasta el clúster de vSAN y, a continuación, haga clic en **Configurar** > **vSAN** > **Servicios**.

2 En Servicios de vSAN, en la fila Servicio de archivos, haga clic en **COMPROBAR ACTUALIZACIÓN**.

3 En el cuadro de diálogo Actualizar servicio de archivos, seleccione una de las siguientes opciones de implementación y, a continuación, haga clic en **ACTUALIZAR**.

Opción	Acción
Método automático	Esta es la opción predeterminada. Esta opción permite que el sistema busque y descargue el archivo OVF. Una vez que se inicie la actualización, no podrá cancelar la tarea. **Nota** vSAN requiere conectividad a Internet para esta opción.
Método manual	Esta opción le permite examinar y seleccionar un archivo OVF que ya esté disponible en el sistema local. Una vez que se inicie la actualización, no podrá cancelar la tarea. **Nota** Si selecciona esta opción, debe cargar los siguientes archivos: ■ `VMware-vSAN-File-Services-Appliance-x.x.x.x-x_OVF10.mf` ■ `VMware-vSAN-File-Services-Appliance-x.x.x.x-x-x_OVF10.cert` ■ `VMware-vSAN-File-Services-Appliance-x.x.x.x-x-x-system.vmdk` ■ `VMware-vSAN-File-Services-Appliance-x.x.x.x-x-cloud-components.vmdk` ■ `VMware-vSAN-File-Services-Appliance-x.x.x.x-x-log.vmdk` ■ `VMware-vSAN-File-Services-Appliance-x.x.x.x-x_OVF10.ovf`

Supervisar el rendimiento del servicio de archivos de vSAN

Puede supervisar el rendimiento de los recursos compartidos de archivos de NFS y SMB.

Requisitos previos

Asegúrese de que el servicio de rendimiento de vSAN esté habilitado. Si utiliza el servicio de rendimiento de vSAN por primera vez, verá un mensaje que informándole de que debe habilitarlo. Para obtener más información sobre el servicio de rendimiento de vSAN, consulte la *Guía de supervisión y solución de problemas de vSAN*.

Procedimiento

1 Desplácese hasta el clúster de vSAN y, a continuación, haga clic en **SUPERVISAR** > **vSAN** > **Rendimiento**.

2 Haga clic en la pestaña **RECURSO COMPARTIDO DE ARCHIVOS**.

3 Seleccione una de las siguientes opciones:

Opción	Acción
Intervalo de tiempo	■ Seleccione **Último** para seleccionar el número de horas para las que desea ver el informe de rendimiento. ■ Seleccione **PERSONALIZADO** para seleccionar la fecha y la hora para las que desea ver el informe de rendimiento. ■ Seleccione **GUARDAR** para agregar la configuración actual como una opción a la lista Intervalo de tiempo.
Recurso compartido de archivos	Seleccione el recurso compartido de archivos para el que desea generar y ver el informe de rendimiento.

4 Haga clic en **MOSTRAR RESULTADOS**.

Resultados

Se mostrarán las métricas de capacidad de proceso, IOPS y latencia del servicio de archivos de vSAN para el período seleccionado.

Para obtener más información sobre los gráficos de rendimiento de vSAN, consulte el artículo de la base de conocimientos de VMware https://kb.vmware.com/s/article/2144493.

Supervisar la capacidad de recursos compartidos de archivos de vSAN

Puede supervisar la capacidad de los recursos compartidos de archivos tanto nativos como administrados por CNS.

Procedimiento

1 Desplácese hasta el clúster de vSAN y, a continuación, haga clic en **SUPERVISAR** > **vSAN** > **Capacidad**.

2 Haga clic en la pestaña **USO DE LA CAPACIDAD**.

3 En la sección Desglose del uso antes de la desduplicación y la compresión, expanda **Objetos de usuario**.

Resultados

Se mostrará la información de capacidad del recurso compartido de archivos.

Para obtener más información sobre la supervisión de la capacidad de vSAN, consulte la *Guía de supervisión y solución de problemas de vSAN*.

Supervisar el estado del recurso compartido de archivos y el servicio de archivos de vSAN

Puede supervisar el estado del servicio de archivos y de los objetos del recurso compartido vSAN de archivos.

Ver el estado del servicio de archivos de vSAN

Puede supervisar el estado del servicio de archivos de vSAN.

Requisitos previos

Asegúrese de que el servicio de rendimiento de vSAN esté habilitado.

Procedimiento

1 Desplácese hasta el clúster de vSAN y, a continuación, haga clic en **Supervisar** > **vSAN**.

2 En la sección Skyline Health, expanda **Servicio de archivos**.

3 Haga clic en los siguientes parámetros de estado del servicio de archivos para ver el estado.

Opción	Acción
Estado de la infraestructura	Muestra el estado de mantenimiento de la infraestructura del servicio de archivos por host ESXi. Para obtener más información, haga clic en la pestaña **Información**.
Estado del servidor de archivos	Muestra el estado de mantenimiento del servidor de archivos. Para obtener más información, haga clic en la pestaña **Información**.
Estado del recurso compartido	Muestra el estado del recurso compartido del servicio de archivos. Para obtener más información, haga clic en la pestaña **Información**.

Supervisar el estado de los objetos de un recurso compartido de archivos de vSAN

Puede supervisar el estado de los objetos de un recurso compartido de archivos.

Para ver el estado de los objetos de un recurso compartido de archivos, vaya al clúster de vSAN y, a continuación, haga clic en **Supervisar** > **vSAN** > **Objetos virtuales**.

La información del dispositivo, como el nombre, el identificador o el UUID, la cantidad de dispositivos que se utilizan para cada máquina virtual y la manera en que se reflejan en todos los hosts se muestra en la sección VER LOS DETALLES DE COLOCACIÓN.

Migrar un clúster híbrido de vSAN a un clúster basado íntegramente en tecnología flash

Puede migrar los grupos de discos de un clúster híbrido de vSAN a grupos de discos basados íntegramente en tecnología flash.

El clúster híbrido de vSAN usa discos magnéticos para la capa de capacidad, y dispositivos flash para la capa de memoria caché. Puede cambiar la configuración de los grupos de discos del clúster de modo que se usen dispositivos flash en la capa de memoria caché y la capa de capacidad.

Nota Siga los pasos para migrar un clúster de vSAN híbrido a una unidad de estado sólido (Solid State Drive, SSD), un clúster de vSAN híbrido a NVMe, o un clúster de SSD a NVMe.

Requisitos previos

- Asegúrese de que todas las directivas de vSAN usadas por el clúster especifiquen **Sin preferencia** para los servicios de cifrado, la eficiencia de espacio y el nivel de almacenamiento.
- Debe usar RAID-1 (creación de reflejo) para **Errores que se toleran** hasta que todos los grupos de discos se conviertan en elementos basados íntegramente en tecnología flash.

  Estos requisitos previos no se aplican cuando se migra un clúster de SSD a NVMe o de NVMe a SSD.

Procedimiento

1 Elimine los grupos de discos híbridos en el host.

   a En vSphere Client, desplácese hasta el clúster de vSAN y haga clic en la pestaña **Configurar**.

   b En vSAN, haga clic en **Administración de discos**.

   c En Grupos de discos, seleccione el grupo de discos que desea eliminar, haga clic en **...** y, a continuación, en **Quitar**.

      Seleccione **Migración de datos completa** como modo de migración y haga clic en **Sí**.

   Nota Migre los grupos de discos en cada uno de los hosts del clúster de vSAN.

   ---

2 Quite los discos HDD físicos del host.

3 Agregue los dispositivos flash al host.

   Compruebe que no haya particiones en los dispositivos flash.

4 Cree los grupos de discos basados íntegramente en tecnología flash en el host.

5 Repita los pasos del 1 al 4 en cada host hasta que todos los grupos de discos híbridos se conviertan en grupos de discos basados íntegramente en tecnología flash.

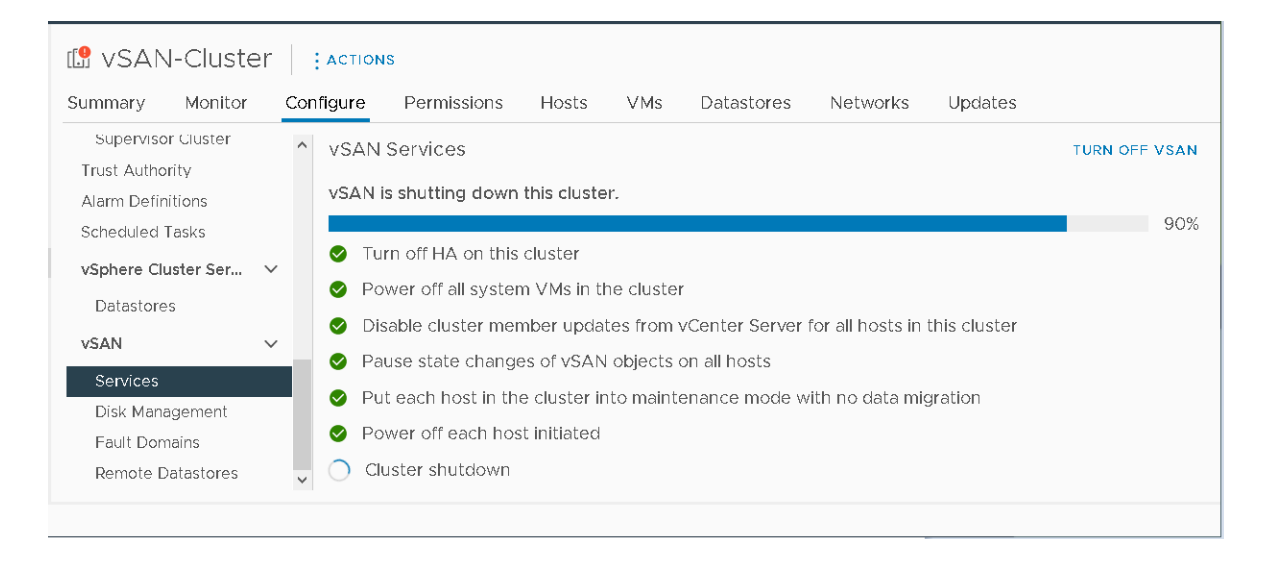
Nota Si no puede conectar discos en caliente en el host, ponga el host en modo de mantenimiento antes de quitar discos en vSphere Client. Apague el host para reemplazar los discos por dispositivos flash. A continuación, encienda el host, salga del modo de mantenimiento y cree nuevos grupos de discos.

Apagar y reiniciar el clúster de vSAN

Puede apagar todo el clúster de vSAN para realizar tareas de mantenimiento o solucionar problemas.

Use el asistente Apagar clúster para apagar el clúster de vSAN. El asistente realizará los pasos necesarios y le avisará cuando requiera la acción del usuario. También puede apagar manualmente el clúster de si es necesario.

Nota Cuando se apaga un clúster ampliado de vSAN, el host testigo permanece activo.



Apagar el clúster de vSAN mediante el asistente Apagar clúster

Utilice el asistente Apagar clúster para apagar correctamente el clúster de vSAN para realizar tareas de mantenimiento o solucionar de problemas.

El asistente Apagar clúster está disponible con vSAN 7.0 Update 3 y versiones posteriores.

Nota Si tiene un entorno de vSphere with Tanzu, debe seguir el orden especificado al apagar o iniciar los componentes. Para obtener más información, consulte "Apagar e iniciar VMware Cloud Foundation" en la *Guía de operaciones de VMware Cloud Foundation*.

Procedimiento

1 Prepare el clúster de vSAN para apagarlo.

   a Compruebe vSAN Skyline Health para confirmar que el clúster está en buen estado.

   b Apague todas las máquinas virtuales almacenadas en el clúster de vSAN, excepto las máquinas virtuales de vCenter Server, de vCLS y del servicio de archivos. Si vCenter Server está alojado en el clúster de vSAN, no apague la máquina virtual de vCenter Server ni las máquinas virtuales de servicio (como DNS o Active Directory) que utiliza vCenter Server.

   c Si se trata de un clúster de servidores de la malla de HCI, apague todas las máquinas virtuales cliente almacenadas en el clúster. Si la máquina virtual de vCenter Server del clúster se clientes está almacenada en este clúster, migre o apague la máquina virtual. Una vez que se apaga este clúster de servidores, los clientes no podrán acceder al almacén de datos compartido.

   d Compruebe que todas las tareas de resincronización se hayan completado.

   Haga clic en la pestaña **Supervisar** y seleccione **vSAN** > **Resincronización de objetos**.

Nota Si algún host miembro está en modo de bloqueo, agregue la cuenta raíz del host a la lista de usuarios con excepción del perfil de seguridad. Para obtener más información, consulte el modo de bloqueo en *Seguridad de vSphere*.

---

2 Haga clic con el botón secundario en el clúster de vSAN en vSphere Client y seleccione el menú **Apagar clúster**.

   También puede hacer clic en **Apagar clúster** en la página Servicios de vSAN.

3 En el asistente Apagar clúster, compruebe que las comprobaciones previas al apagado estén en color verde. Resuelva los problemas con exclamaciones de color rojo. Haga clic en **Siguiente**.

   Si el dispositivo de vCenter Server se implementa en el clúster de vSAN, el asistente Apagar clúster mostrará el aviso vCenter Server. Anote la dirección IP del host de orquestación, en caso de que lo necesite durante el reinicio del clúster. Si vCenter Server utiliza máquinas virtuales de servicio como DNS o Active Directory, márquelas como máquinas virtuales excepcionales en el asistente Apagar clúster.

4 Introduzca un motivo para realizar el apagado y haga clic en **Apagar**.

   La página Servicios de vSAN cambiará para mostrar información sobre el proceso de apagado.

5 Supervise el proceso de apagado.

   vSAN realizará los pasos necesarios para apagar el clúster, las máquinas virtuales del sistema y los hosts.

Pasos siguientes

Reinicie el clúster de vSAN. Consulte Reiniciar el clúster de vSAN.

Reiniciar el clúster de vSAN

Puede reiniciar un clúster de vSAN que esté apagado para realizar tareas mantenimiento o solucionar problemas.

Procedimiento

1 Encienda los hosts del clúster.

Si vCenter Server está alojado en el clúster vSAN, espere a que se reinicie vCenter Server.

2 Haga clic con el botón secundario en el clúster de vSAN en vSphere Client y seleccione el menú **Reiniciar clúster**.

También puede hacer clic en **Reiniciar clúster** en la página Servicios de vSAN.

3 En el cuadro de diálogo Reiniciar clúster, haga clic en **Reiniciar**.

La página Servicios de vSAN cambiará para mostrar información sobre el proceso de reinicio.

4 Después de reiniciar el clúster, compruebe vSAN Skyline Health y resuelva los problemas pendientes.

Apagar y reiniciar manualmente el clúster de vSAN

Puede apagar manualmente todo el clúster de vSAN para realizar tareas de mantenimiento o solucionar problemas.

Utilice el asistente Apagar clúster a no ser que el flujo de trabajo requiera un apagado manual. Cuando apague manualmente el clúster de vSAN, no desactive vSAN en el clúster.

Nota Si tiene un entorno de vSphere with Tanzu, debe seguir el orden especificado al apagar o iniciar los componentes. Para obtener más información, consulte "Apagar e iniciar VMware Cloud Foundation" en la *Guía de operaciones de VMware Cloud Foundation*.

Procedimiento

1 Apague el clúster de vSAN.

   a Compruebe vSAN Skyline Health para confirmar que el clúster está en buen estado.

   b Apague todas las máquinas virtuales que se ejecutan en el clúster de vSAN si vCenter Server no está alojado en el clúster. Si vCenter Server está alojado en el clúster de vSAN, no apague la máquina virtual de vCenter Server ni las máquinas virtuales de servicio (como DNS o Active Directory) que utiliza vCenter Server.

c Si el servicio de archivos de vSAN está habilitado en el clúster de vSAN, deberá desactivarlo. Al desactivar el servicio de archivos de vSAN, se eliminará el dominio del servicio de archivos vacío. Si desea conservar el dominio del servicio de archivos vacío después de reiniciar el clúster de vSAN, debe crear un recurso compartido de archivos NFS o SMB antes de desactivar el servicio de archivos de vSAN.

d Haga clic en la pestaña **Configurar** y desactive HA. Como resultado, el clúster no registrará apagados de hosts como errores.

Para vSphere 7.0 U1 y versiones posteriores, habilite el modo de retirada de vCLS. Para obtener más información, consulte el artículo de la base de conocimientos de VMware en https://kb.vmware.com/s/article/80472.

e Compruebe que todas las tareas de resincronización se hayan completado.

Haga clic en la pestaña **Supervisar** y seleccione **vSAN** > **Resincronización de objetos**.

f Si vCenter Server está alojado en el clúster de vSAN, apague la máquina virtual de vCenter Server.

Tome nota del host que ejecuta la máquina virtual vCenter Server. Es el host en el que se debe reiniciar la máquina virtual de vCenter Server.

g Desactive las actualizaciones de miembros del clúster desde vCenter Server ejecutando el siguiente comando en los hosts de ESXi del clúster. Asegúrese de ejecutar el siguiente comando en todos los hosts.

```
esxcfg-advcfg -s 1 /VSAN/IgnoreClusterMemberListUpdates
```

h Inicie sesión en cualquier host del clúster que no sea el host testigo.

i Ejecute el siguiente comando solo en ese host. Si ejecuta el comando en varios hosts a la vez, puede provocar que una condición de carrera cause resultados inesperados.

```
python /usr/lib/vmware/vsan/bin/reboot_helper.py prepare
```

El comando devuelve e imprime lo siguiente:

```
Se realizó la preparación del clúster.
```

Nota

- El clúster está totalmente particionado después de que el comando se haya completado correctamente.
- Si se produce un error, solucione el problema en función del mensaje de error y vuelva a habilitar el modo de retirada de vCLS.
- Si hay hosts desconectados o en mal estado en el clúster, quite los hosts y vuelva a intentar ejecutar el comando.

j Coloque todos los hosts en modo de mantenimiento con **Sin acción**. Si vCenter Server está apagado, use el siguiente comando para colocar los hosts de ESXi en el modo de mantenimiento con **Sin acción**.

```
esxcli system maintenanceMode set -e true -m noAction
```

Realice este paso en todos los hosts.

Para evitar el riesgo de falta de disponibilidad de datos al utilizar **Sin acción** al mismo tiempo en varios hosts, y después de reiniciar varios hosts, consulte este artículo de la base de conocimientos de VMware: https://kb.vmware.com/s/article/60424. Para realizar un reinicio simultáneo de todos los hosts del clúster mediante una herramienta integrada, consulte este artículo de la base de conocimientos de VMware: https://kb.vmware.com/s/article/70650.

k Después de que todos los hosts hayan entrado correctamente en el modo de mantenimiento, realice las tareas de mantenimiento necesarias y apague los hosts.

2 Reinicie el clúster de vSAN.

a Encienda los hosts ESXi.

Encienda el cuadro físico en el que está instalado ESXi. El host de ESXi se inicia, busca las máquinas virtuales correspondientes y funciona con normalidad.

Si algún host no se reinician, deberá recuperarlo de forma manual o moverlo fuera del clúster de vSAN.

b Cuando todos los hosts vuelvan a encenderse, salga del modo de mantenimiento en todos los hosts. Si vCenter Server está apagado, use el siguiente comando en los hosts de ESXi para salir del modo de mantenimiento.

```
esxcli system maintenanceMode set -e false
```

Realice este paso en todos los hosts.

c Inicie sesión en uno de los hosts del clúster que no sean el host testigo.

d Ejecute el siguiente comando solo en ese host. Si ejecuta el comando en varios hosts a la vez, puede provocar que una condición de carrera cause resultados inesperados.

```
python /usr/lib/vmware/vsan/bin/reboot_helper.py recover
```

El comando devuelve e imprime lo siguiente:

`El reinicio o encendido del clúster se completó correctamente.`

e Compruebe que todos los hosts estén disponibles en el clúster ejecutando el siguiente comando en cada host.

```
esxcli vsan cluster get
```

f Habilite las actualizaciones de miembros del clúster desde vCenter Server ejecutando el siguiente comando en los hosts de ESXi del clúster. Asegúrese de ejecutar el siguiente comando en todos los hosts.

```
esxcfg-advcfg -s 0 /VSAN/IgnoreClusterMemberListUpdates
```

g Reinicie la máquina virtual de vCenter Server si está apagada. Espere a que la máquina virtual de vCenter Server se encienda y se ejecute. Para desactivar el modo de retirada de vCLS, consulte el artículo de la base de conocimiento de VMware en https://kb.vmware.com/s/article/80472.

h Compruebe que todos los hosts estén disponibles en el clúster de vSAN ejecutando el siguiente comando en cada host.

```
esxcli vsan cluster get
```

i Reinicie las máquinas virtuales restantes a través de vCenter Server.

j Compruebe vSAN Skyline Health y resuelva los problemas pendientes.

k (Opcional) Habilite el servicio de archivos de vSAN.

l (Opcional) Si el clúster de vSAN tiene habilitada Disponibilidad de vSphere, debe reiniciar manualmente Disponibilidad de vSphere para evitar el siguiente error: `No se puede encontrar el agente principal de vSphere HA`.

Para reiniciar de forma manual Disponibilidad de vSphere, seleccione el clúster de vSAN y acceda a:

1 **Configurar** > **Servicios** > **Disponibilidad de vSphere** > **EDITAR** > **Deshabilitar vSphere HA**

2 **Configurar** > **Servicios** > **Disponibilidad de vSphere** > **EDITAR** > **Habilitar vSphere HA**

3 Si hay hosts desconectados o en mal estado en el clúster, recupere o quite los hosts del clúster de vSAN. Si vCenter Server utiliza máquinas virtuales de servicio como DNS o Active Directory, márquelas como máquinas virtuales excepcionales en el asistente Apagar clúster.

Vuelva a intentar los comandos anteriores solo después de que vSAN Skyline Health muestre todos los hosts disponibles en estado verde.

Si tiene un clúster de vSAN de tres nodos, el comando `reboot_helper.py recover` no puede funcionar en una situación de error de un host. Como administrador, haga lo siguiente:

a Quite temporalmente la información del host de error de la lista de agentes de unidifusión.

b Agregue el host después de ejecutar el siguiente comando.

```
reboot_helper.py recover
```

A continuación, se muestran los comandos para quitar y agregar el host a un clúster de vSAN:

```
#esxcli vsan cluster unicastagent remove -a <IP Address> -t node -u <NodeUuid>
```

```
#esxcli vsan cluster unicastagent add -t node -u <NodeUuid> -U true -a <IP Address> -p
12321
```

Pasos siguientes

Reinicie el clúster de vSAN. Consulte Reiniciar el clúster de vSAN.

Administrar dispositivos en un clúster de vSAN

9

Puede realizar varias tareas de administración de dispositivos en un clúster de vSAN.

Puede crear grupos de discos híbridos o basados íntegramente en tecnología flash, habilitar vSAN para reclamar dispositivos para memoria caché y capacidad, activar o desactivar los indicadores LED, marcar dispositivos como flash, marcar dispositivos remotos como locales, etc.

Nota No se pueden marcar dispositivos como flash ni marcar dispositivos remotos como locales en un clúster de vSAN Express Storage Architecture.

Lea los siguientes temas a continuación:

Administrar dispositivos de almacenamiento en un clúster de vSAN

Cuando configure vSAN en un clúster, reclame dispositivos de almacenamiento en cada host para crear el almacén de datos de vSAN.

El clúster de vSAN contiene inicialmente un único almacén de datos de vSAN. A medida que reclama discos para grupos de discos o grupos de almacenamiento en cada host, el tamaño del almacén de datos aumenta en función de la cantidad de capacidad física que agregaron estos dispositivos.

vSAN tiene un flujo de trabajo uniforme para reclamar discos en todos los escenarios. Puede ver todos los discos disponibles por modelo y tamaño o por host.

Agregar un grupo de discos (vSAN Original Storage Architecture)

Al agregar un grupo de discos, debe especificar el host y los dispositivos que se reclamarán. Cada grupo de discos contiene un dispositivo flash de almacenamiento en caché y uno o varios dispositivos de capacidad. Puede crear varios grupos de discos en cada host y reclamar un dispositivo de memoria caché para cada grupo de discos.

Cuando agregue un grupo de discos, tenga en cuenta la proporción entre el almacenamiento en caché flash y la capacidad consumida. La proporción depende de los requisitos y de la carga de trabajo del clúster. En un clúster híbrido, considere utilizar al menos un 10 % de memoria caché flash para la proporción de capacidad utilizada (sin incluir réplicas, como duplicados).

Nota Si se agrega un nuevo host ESXi al clúster de vSAN, el almacenamiento local de ese host no se agrega automáticamente al almacén de datos de vSAN. Debe agregar un grupo de discos para utilizar el almacenamiento del nuevo host.

Agregar un grupo de almacenamiento (vSAN Express Storage Architecture)

Cada host que aporta almacenamiento contiene un solo grupo de almacenamiento de dispositivos flash. Cada dispositivo flash proporciona caché y capacidad al clúster. Puede agregar un grupo de almacenamiento mediante cualquier dispositivo compatible. vSAN crea un solo grupo de almacenamiento por host, independientemente de la cantidad de discos de almacenamiento a los que está asociado el host.

Reclamar discos para vSAN Direct

Utilice vSAN Direct para permitir que los servicios con estado accedan al almacenamiento local sin procesar ajeno a vSAN a través de una ruta directa.

Puede reclamar dispositivos locales de host para vSAN Direct y utilizar vSAN para administrar y supervisar dichos dispositivos. En cada dispositivo local, vSAN Direct crea un almacén de datos VMFS independiente y lo pone a disposición de la aplicación con estado.

Cada almacén de datos de vSAN Direct aparece como un almacén de datos vSAN-D.

Nota Si vSAN Express Storage Architecture está habilitado para el clúster, no podrá reclamar discos para vSAN Direct.

Crear un grupo de discos o un grupo de almacenamiento en un clúster de vSAN

En función de la arquitectura de almacenamiento que utilice en el clúster, puede optar por crear un grupo de discos o un grupo de almacenamiento.

Crear un grupo de discos en un host (vSAN Original Storage Architecture)

Puede reclamar dispositivos de memoria caché y capacidad para definir grupos de discos en un host de vSAN. Seleccione un dispositivo de caché y uno o varios dispositivos de capacidad para crear el grupo de discos.

1. Navegar hacia el clúster de vSAN.
2. Haga clic en la pestaña **Configurar**.
3. En vSAN, haga clic en **Administración de discos**, seleccione un host de la tabla y haga clic en **VER DISCOS**.

4 Haga clic en **CREAR GRUPO DE DISCOS**.

5 Seleccione los discos que se reclamarán.

   a Seleccione el dispositivo Flash que se utilizará para el nivel de memoria caché.

   b Seleccione los discos que se usarán para el nivel de capacidad.

   7. Haga clic en **Crear** para confirmar sus selecciones.

   Nota El nuevo grupo de discos se muestra en la lista.

Crear un grupo de almacenamiento en un host (vSAN Express Storage Architecture)

Puede reclamar discos para definir un grupo de almacenamiento en un host de vSAN. Cada host que aporta almacenamiento contiene un solo grupo de almacenamiento de dispositivos flash. Cada dispositivo flash proporciona caché y capacidad al clúster. Puede crear un grupo de almacenamiento con cualquier dispositivo que sea compatible con ESA. vSAN crea solo un grupo de almacenamiento por host.

En un grupo de almacenamiento, cada dispositivo proporciona almacenamiento en caché y capacidad en un solo nivel. Eso es diferente de un grupo de discos, que tiene dispositivos dedicados en diferentes niveles de memoria caché y capacidad.

Utilice la reclamación de disco administrado de vSAN para reclamar automáticamente todos los discos compatibles en los hosts del clúster. Al agregar nuevos hosts, vSAN también reclamará discos compatibles en esos hosts. Este ajuste no afecta a los discos agregados manualmente. Puede agregar manualmente dichos discos al grupo de almacenamiento.

1 Desplácese hasta el clúster de vSAN.

2 Haga clic en la pestaña **Configurar**.

3 En vSAN, haga clic en **Administración de discos**.

4 Haga clic en **Reclamar discos sin utilizar**.

   Nota Puede cambiar el modo de reclamación de disco para utilizar **Reclamación de disco administrado de vSAN**. vSAN reclamará automáticamente todos los dispositivos compatibles en los hosts del clúster.

5 Agrupe por host.

6 Seleccione los discos compatibles que se reclamarán.

7 Haga clic en **Crear** para confirmar sus selecciones.

   Nota Aparecerá la página de administración de discos con los hosts enumerados. Se indicará que se reclamarán discos en los hosts en la columna "Discos en uso", que refleja el número actualizado de discos por host. Para ver los discos reclamados para el host, haga clic en el botón "Ver discos".

Reclamar dispositivos de almacenamiento para un clúster de vSAN Original Storage Architecture

Puede seleccionar un grupo de dispositivos de capacidad y de memoria caché. vSAN los organizará en grupos de discos predeterminados.

En este método se seleccionan dispositivos para crear grupos de discos para el clúster de vSAN. Necesitará un dispositivo de almacenamiento en caché y, al menos, un dispositivo de capacidad para cada grupo de discos.

Procedimiento

1. Desplácese hasta el clúster de vSAN.
2. Haga clic en la pestaña **Configurar**.
3. En vSAN, haga clic en **Administración de discos**.
4. Haga clic en **Reclamar discos sin utilizar**.
5. Seleccione los dispositivos que se agregarán a los grupos de discos.
   - Para los grupos de discos híbridos, cada host que aporta almacenamiento debe aportar un dispositivo flash de memoria caché, así como uno o varios dispositivos de capacidad HDD. Puede agregar un solo dispositivo de memoria caché por grupo de discos.
     - Seleccione el dispositivo flash que se utilizará como memoria caché y haga clic en **Reclamar por nivel de memoria caché**.
     - Seleccione uno o varios dispositivos HDD para usarlos como capacidad y haga clic en **Reclamar por nivel de capacidad** para cada uno de ellos.
     - Haga clic en **Crear** o en **Aceptar**.
   - Para los grupos de discos basados en flash, cada host que aporta almacenamiento debe aportar un dispositivo flash de memoria caché, así como uno o varios dispositivos de capacidad flash. Puede agregar un solo dispositivo de memoria caché por grupo de discos.
     - Seleccione uno o varios dispositivos flash para usarlos como memoria caché y haga clic en **Reclamar por nivel de memoria caché** para acceder a ellos.
     - Seleccione el dispositivo flash que se utilizará para capacidad y haga clic en **Reclamar por nivel de capacidad**.
     - Haga clic en **Crear** o en **Aceptar**.

   vSAN reclama los dispositivos seleccionados y los organiza en grupos de discos predeterminados que contribuyen al almacén de datos de vSAN.

Para comprobar la función de cada dispositivo agregado al grupo de discos basado íntegramente en tecnología flash, desplácese hasta la columna "Reclamado como" de un host determinado en la página Administración de discos. La tabla muestra la lista de dispositivos y su función en un grupo de discos. Para los grupos de discos híbridos y basados íntegramente en tecnología flash, el disco de memoria caché siempre se mostrará en primer lugar en la cuadrícula del grupo de discos.

Reclamar dispositivos de almacenamiento para un clúster de vSAN Express Storage Architecture

Puede seleccionar un grupo de dispositivos de un host y vSAN los organizará en un grupo de almacenamiento.

Después de habilitar vSAN ESA, puede reclamar discos de forma manual o automática. Con el método manual, podrá seleccionar un grupo de dispositivos de almacenamiento para reclamarlo.

En la reclamación automática de discos, vSAN seleccionará automáticamente todos los discos compatibles de los hosts. Cuando se agregan hosts nuevos al clúster, vSAN reclama automáticamente los discos compatibles disponibles en esos hosts y agrega el almacenamiento al almacén de datos de vSAN.

Puede elegir dispositivos que no se notifiquen como certificados para vSAN ESA, y esos dispositivos se tendrán en cuenta en el grupo de almacenamiento, pero esta configuración no es recomendable y puede afectar el rendimiento.

Procedimiento

1. Desplácese hasta el clúster de vSAN.
2. Haga clic en la pestaña **Configurar**.
3. En vSAN, haga clic en **Administración de discos**.
4. Para reclamar discos manualmente, haga clic en **Reclamar discos sin utilizar**.
   a. Seleccione los dispositivos que desea reclamar
   b. Haga clic en **Crear**.
5. Para reclamar discos automáticamente, haga clic en **CAMBIAR MODO DE RECLAMACIÓNDE DISCO** y haga clic en el botón de alternancia **Reclamación de disco administrado de vSAN**.

   Nota Si opta por utilizar la recuperación de discos administrados por vSAN al configurar el clúster, el botón de alternancia ya estará habilitado.

   vSAN reclama los dispositivos seleccionados y los organiza en grupos de almacenamiento que respaldan el almacén de datos de vSAN. De forma predeterminada, vSAN creará un grupo de almacenamiento para cada host ESXi que aporta almacenamiento al clúster. Si los dispositivos seleccionados no están certificados para vSAN ESA, dichos dispositivos no se tendrán en cuenta para la creación de grupos de almacenamiento.

Reclamar discos para vSAN Direct

Puede reclamar dispositivos de almacenamiento local como vSAN Direct para usarlos con la plataforma de persistente de datos de vSAN.

Nota Solo la plataforma de persistencia de datos de vSAN puede consumir almacenamiento de vSAN Direct. La plataforma de persistencia de datos de vSAN proporciona un marco para que los partners de tecnología de software se integren con la infraestructura de VMware. Cada socio debe desarrollar su propio complemento para que los clientes de VMware reciban los beneficios de la plataforma de persistencia de datos de vSAN. La plataforma no funcionará hasta que la solución del partner que se ejecuta en la parte superior esté operativa. Para obtener más información, consulte *Administración y configuración de vSphere con Tanzu*.

Procedimiento

1 En vSphere Client, desplácese hasta el clúster de vSAN.

2 Haga clic en la pestaña **Configurar**.

3 En vSAN, haga clic en **Administración de discos**.

4 Haga clic en **Reclamar discos sin utilizar**.

5 En el cuadro de diálogo Reclamar discos sin utilizar, seleccione la pestaña vSAN Direct.

6 Para seleccionar un dispositivo para reclamarlo, marque la casilla situada en la columna **Reclamación de vSAN Direct**.

   Nota Los dispositivos reclamados para su clúster de vSAN no aparecen en la pestaña vSAN Direct.

7 Haga clic en **Crear**.

Resultados

Por cada dispositivo que reclame, vSAN creará un nuevo almacén de datos de vSAN Direct.

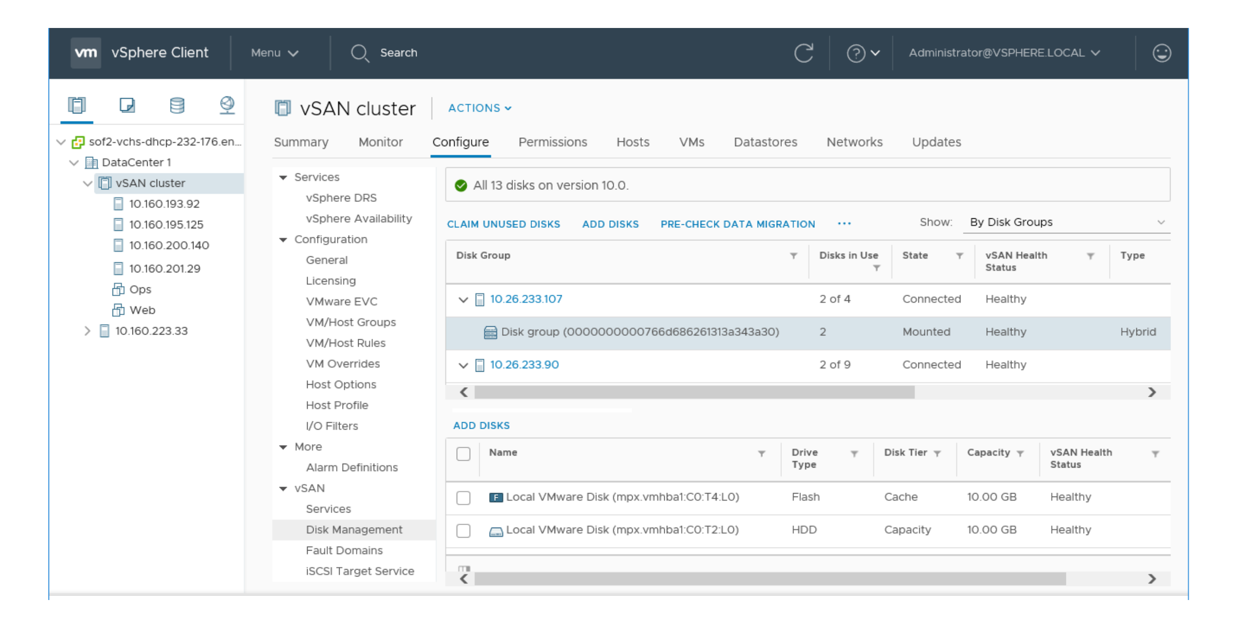
Pasos siguientes

Puede hacer clic en la pestaña Almacenes de datos para mostrar todos los almacenes de datos de vSAN Direct de su clúster.

Trabajar con dispositivos individuales en un clúster de vSAN

Puede realizar varias tareas de administración de dispositivos en el clúster de vSAN.

Puede agregar dispositivos a un grupo de discos, quitar dispositivos de un grupo de discos, habilitar o deshabilitar los LED del localizador y marcar dispositivos. También puede agregar o quitar discos reclamados mediante vSAN Direct.



Agregar dispositivos al grupo de discos en un clúster de vSAN

Cuando configura vSAN para reclamar discos en modo manual, puede agregar dispositivos locales adicionales a los grupos de discos existentes.

Los dispositivos deben ser del mismo tipo que los dispositivos existentes en los grupos de discos, como discos de estado sólido (SSD) o discos magnéticos.

Procedimiento

1 Desplácese hasta el clúster de vSAN.

2 Haga clic en la pestaña **Configurar**.

3 En vSAN, haga clic en **Administración de discos**.

4 Seleccione el grupo de discos y haga clic en **Agregar discos**.

5 Seleccione el dispositivo que desea agregar y haga clic en **Agregar**.

Si agrega un dispositivo usado que contiene información de particiones o datos residuales, en primer lugar debe limpiar el dispositivo. Para conocer cuál es el procedimiento para quitar información de particiones de los dispositivos, consulte Quitar particiones de dispositivos. También es posible ejecutar el comando de RVC `host_wipe_vsan_disks` para aplicar formato al dispositivo.

Pasos siguientes

Verifique que la comprobación de estado del equilibrio de disco de vSAN sea de color verde. Si la comprobación de estado del equilibrio de disco emite una advertencia, ejecute una operación de reequilibrio automático fuera de las horas punta. Para obtener más información, consulte "Configurar el reequilibrio automático en un clúster de vSAN" en *Supervisar vSAN y solucionar sus problemas*.

Comprobar las capacidades de migración de datos de un disco o un grupo de discos de un clúster de vSAN

Utilice la comprobación previa de migración de datos para averiguar el impacto de las opciones de migración al desmontar un disco o un grupo de discos, o al quitarlo del clúster de vSAN.

Ejecute la comprobación previa de migración de datos antes de desmontar o quitar un disco o un grupo de discos del clúster de vSAN. Los resultados de la prueba proporcionarán información para determinar el impacto sobre la capacidad del clúster, las comprobaciones de estado previsto y los objetos que se apartarán del cumplimiento. Si se espera que la operación no se realice correctamente, la comprobación previa proporcionará información sobre los recursos necesarios.

Procedimiento

1 Desplácese hasta el clúster de vSAN.

2 Haga clic en la pestaña Supervisar.

3 En vSAN, haga clic en **Comprobación previa a la migración de datos**.

4 Seleccione un disco o un grupo de discos, elija una opción de migración de datos y haga clic en **Comprobación previa**.

   vSAN ejecutará las pruebas de comprobación previa de migración de datos.

5 Vea los resultados de la prueba.

   Los resultados de la comprobación previa mostrarán si puede desmontar o quitar el disco o el grupo de discos de forma segura.

   - La pestaña Conformidad y accesibilidad de objetos muestra los objetos que pueden presentar problemas después de la migración de datos.
   - La pestaña Capacidad del clúster muestra el impacto de la migración de datos en el clúster de vSAN antes y después de realizar la operación.
   - La pestaña Estado previsto muestra las comprobaciones de estado que podrían verse afectadas por la migración de datos.

Pasos siguientes

Si la comprobación previa indica que puede desmontar o quitar el dispositivo, haga clic en la opción para continuar con la operación.

Quitar grupos de discos o dispositivos de vSAN

Puede quitar dispositivos seleccionados del grupo de discos o puede quitar un grupo de discos completo de un clúster de vSAN OSA.

Dado que quitar dispositivos no protegidos puede ser un proceso disruptivo para el almacén de datos de vSAN y las máquinas virtuales del almacén de datos, evite quitar dispositivos o grupos de discos.

Por lo general, se quitan dispositivos o grupos de discos de vSAN cuando se actualiza un dispositivo o se reemplaza un dispositivo con errores, o cuando se debe quitar un dispositivo de memoria caché. Otras características de almacenamiento de vSphere pueden usar cualquier dispositivo basado en flash que se quite del clúster de vSAN.

La eliminación permanente de un grupo de discos elimina los miembros del disco y los datos almacenados en los dispositivos.

Nota Al quitar un dispositivo flash de almacenamiento en caché o todos los dispositivos de capacidad de un grupo de discos, se quita el grupo de discos completo.

Nota Si el clúster de utiliza desduplicación y compresión, no podrá quitar un solo disco del grupo de discos. Debe quitar el grupo de discos completo.

La evacuación de datos de dispositivos o grupos de discos puede ocasionar un incumplimiento temporal de las directivas de almacenamiento de máquinas virtuales.

Requisitos previos

Ejecute la comprobación previa de migración de datos en el dispositivo o el grupo de discos antes de quitarlo del clúster. Para obtener más información, consulte

Procedimiento

1 Desplácese hasta el clúster de vSAN.

2 Haga clic en la pestaña **Configurar**.

3 En vSAN, haga clic en **Administración de discos**.

4 Quite el grupo de discos o los dispositivos seleccionados.

Opción	Descripción
Quitar el grupo de discos	a En Grupos de discos, seleccione el grupo de discos que desea eliminar, haga clic en **...** y, a continuación, haga clic en **Quitar**. b Seleccione un modo de evacuación de datos.
Quitar el dispositivo seleccionado	a En Grupos de discos, seleccione el grupo de discos que contiene el dispositivo que desea quitar. b En Discos, seleccione el dispositivo que desea eliminar y haga clic en el icono **Quitar discos**. c Seleccione un modo de evacuación de datos.

5 Haga clic en **Sí** o en **Quitar** para confirmar.

Los datos se evacúan de los dispositivos seleccionados o de un grupo de discos.

Volver a crear un grupo de discos en un clúster de vSAN

Cuando se vuelve a crear un grupo de discos en el clúster de vSAN, los discos existentes se quitan del grupo de discos y este se elimina.

vSAN vuelve a crear el grupo de discos con los mismos discos. Cuando se vuelve a crear un grupo de discos en un clúster de vSAN, vSAN administra el proceso por usted. vSAN evacua los datos de todos los discos en el grupo de discos, quita el grupo de discos y crea el grupo de discos con los mismos discos.

Procedimiento

1 Desplácese hasta el clúster de vSAN en vSphere Client.

2 Haga clic en la pestaña **Configurar**.

3 En vSAN, haga clic en **Administración de discos**.

4 En Grupos de discos, seleccione el grupo de discos que desea volver a crear.

5 Haga clic en **...** y, a continuación, haga clic en **Volver a crear**.

Aparece el cuadro de diálogo Volver a crear grupo de discos.

6 Seleccione un modo de migración de datos y haga clic en **Volver a crear**.

Resultados

Se evacuan todos los datos que residen en los discos. El grupo de discos se elimina del clúster y se vuelve a crear.

Usar los LED del localizador en vSAN

No puede usar los LED del localizador para identificar la ubicación de los dispositivos de almacenamiento.

vSAN puede encender el LED del localizador en un dispositivo con errores a fin de que pueda identificar fácilmente el dispositivo. Esto resulta especialmente útil al trabajar con varios escenarios de conexión e intercambio en caliente.

Considere utilizar controladores de almacenamiento de E/S con el modo de paso, debido a que los controladores con el modo RAID 0 requieren pasos adicionales para habilitar el reconocimiento de los controladores de los LED del localizador.

Para obtener información sobre la configuración de los controladores de almacenamiento en modo RAID 0, consulte la documentación del proveedor.

LED del localizador

Puede activar o desactivar los LED del localizador de los dispositivos de almacenamiento de vSAN. Cuando active el LED del localizador, puede identificar la ubicación de un dispositivo de almacenamiento específico.

Cuando ya no necesite una alerta visual de los dispositivos de vSAN, puede desactivar los LED del localizador en los dispositivos seleccionados.

Requisitos previos

- Compruebe que haya instalado los controladores compatibles para las controladoras de E/S de almacenamiento que habilitan esta característica. Para obtener información sobre los controladores que están certificados por VMware, consulte la *Guía de compatibilidad de VMware* en la URL: http://www.vmware.com/resources/compatibility/search.php.
- En algunos casos, es posible que necesite usar utilidades de otros fabricantes para configurar la característica de los LED del localizador en las controladoras de E/S de almacenamiento. Por ejemplo, al usar HP, debe comprobar que esté instalada la CLI de HP SSA.

Para obtener más información sobre la instalación de VIB de otros fabricantes, consulte el documento *Actualización de vSphere*.

Procedimiento

1 Desplácese hasta el clúster de vSAN.

2 Haga clic en la pestaña **Configurar**.

3 En vSAN, haga clic en **Administración de discos**.

4 Seleccione un host para ver la lista de dispositivos.

5 En la parte inferior de la página, seleccione uno o varios dispositivos de almacenamiento o más de la lista, y realice la acción deseada para los LED del localizador.

Opción	Acción
Encender LED	Activa el LED del localizador en el dispositivo de almacenamiento seleccionado. También puede usar la pestaña **Administrar** y hacer clic en **Almacenamiento > Dispositivos de almacenamiento**.
Apagar LED	Desactiva el LED del localizador en el dispositivo de almacenamiento seleccionado. También puede usar la pestaña **Administrar** y hacer clic en **Almacenamiento > Dispositivos de almacenamiento**.

Marcar dispositivos como dispositivos flash en vSAN

Cuando los hosts ESXi no identifican automáticamente los dispositivos flash como tales, puede marcarlos manualmente como dispositivos flash locales.

Es posible que los dispositivos flash no se reconozcan como flash cuando admiten el modo RAID 0 en lugar del modo de acceso directo. Cuando los dispositivos no se reconocen como dispositivos flash locales, se excluyen de la lista de dispositivos que se ofrecen para vSAN y no es posible utilizarlos en el clúster de vSAN. Cuando estos dispositivos se marcan como dispositivos flash locales, pasan a estar disponibles para vSAN.

Requisitos previos

- Compruebe que el dispositivo sea local para el host.
- Compruebe que el dispositivo no esté en uso.

- Asegúrese de que las máquinas virtuales que acceden al dispositivo estén apagadas y de que el almacén de datos esté desmontado.

Procedimiento

1. Desplácese hasta el clúster de vSAN.
2. Haga clic en la pestaña **Configurar**.
3. En vSAN, haga clic en **Administración de discos**.
4. Seleccione el host para ver la lista de dispositivos disponibles.
5. Desde el menú desplegable **Mostrar**, ubicado en la parte inferior de la página, seleccione **No en uso**.
6. Seleccione uno o varios dispositivos flash de la lista y haga clic en **Marcar como disco flash**.
7. Haga clic en **Sí** para guardar los cambios.

   El tipo de unidad de los dispositivos seleccionados aparecerá como Flash.

Marcar dispositivos como discos HDD en vSAN

Cuando los hosts ESXi no identifican automáticamente los discos magnéticos locales como dispositivos HDD, puede marcarlos manualmente como dispositivos HDD locales.

Si ha marcado un disco magnético como dispositivo flash, puede cambiar el tipo de disco del dispositivo marcándolo como disco magnético.

Requisitos previos

- Compruebe que el disco magnético sea local para el host.
- Compruebe que el disco magnético no esté en uso y que esté vacío.
- Compruebe que las máquinas virtuales que acceden al dispositivo estén apagadas.

Procedimiento

1. Desplácese hasta el clúster de vSAN.
2. Haga clic en la pestaña **Configurar**.
3. En vSAN, haga clic en **Administración de discos**.
4. Seleccione el host para ver la lista de dispositivos magnéticos disponibles.
5. Desde el menú desplegable **Mostrar**, ubicado en la parte inferior de la página, seleccione **No en uso**.
6. Seleccione uno o varios discos magnéticos en la lista y haga clic en **Marcar como disco HDD**.
7. Haga clic en **Sí** para guardar.

   El tipo de unidad de los discos magnéticos seleccionados aparece como HDD.

Marcar dispositivos como locales en vSAN

Cuando los hosts usan gabinetes SAS externos, es posible que vSAN reconozca ciertos dispositivos como remotos y que no pueda reclamarlos de manera automática como locales.

En dichos casos, puede indicar que los dispositivos son locales.

Requisitos previos

Asegúrese de que el dispositivo de almacenamiento no sea un dispositivo compartido.

Procedimiento

1 Desplácese hasta el clúster de vSAN.
2 Haga clic en la pestaña **Configurar**.
3 En vSAN, haga clic en **Administración de discos**.
4 Seleccione un host para ver la lista de dispositivos.
5 Desde el menú desplegable **Mostrar**, ubicado en la parte inferior de la página, seleccione **No en uso**.
6 En la lista de dispositivos, seleccione el o los dispositivos remotos que desee marcar como locales y haga clic en **Marcar como disco local**.
7 Haga clic en **Sí** para guardar los cambios.

Marcar dispositivos como remotos en vSAN

Los hosts que usan controladores SAS externos pueden compartir dispositivos.

Esos dispositivos compartidos pueden marcarse manualmente como remotos, de modo que vSAN no reclame los dispositivos al crear grupos de discos. En vSAN, no es posible agregar dispositivos compartidos a un grupo de discos.

Procedimiento

1 Desplácese hasta el clúster de vSAN.
2 Haga clic en la pestaña **Configurar**.
3 En vSAN, haga clic en **Administración de discos**.
4 Seleccione un host para ver la lista de dispositivos.
5 Desde el menú desplegable **Mostrar**, ubicado en la parte inferior de la página, seleccione **No en uso**.
6 Seleccione el o los dispositivos que desee marcar como remotos y haga clic en **Marcar como remoto**.
7 Haga clic en **Sí** para confirmar.

Agregar un dispositivo de capacidad a un grupo de discos de vSAN

Es posible agregar un dispositivo de capacidad a un grupo de discos de vSAN existente.

No es posible agregar dispositivos compartidos a un grupo de discos.

Requisitos previos

Compruebe que el dispositivo no tenga formato y no esté en uso.

Procedimiento

1 Desplácese hasta el clúster de vSAN.

2 Haga clic en la pestaña **Configurar**.

3 En vSAN, haga clic en **Administración de discos**.

4 Seleccione un grupo de discos.

5 Haga clic en **Agregar discos** en la parte inferior de la página.

6 Seleccione el dispositivo de capacidad que desea agregar al grupo de discos.

7 Haga clic en **Aceptar** o en **Agregar**.

   El dispositivo se agregará al grupo de discos.

Quitar particiones de dispositivos

Puede quitar la información de particiones de un dispositivo a fin de que vSAN pueda reclamar el dispositivo y utilizarlo.

Si ha agregado un dispositivo que contiene información de particiones o datos residuales, debe quitar toda la información de particiones previa del dispositivo antes de reclamarlo para utilizarlo con vSAN. VMware recomienda agregar dispositivos limpios a los grupos de discos.

Al quitar información de particiones de un dispositivo, vSAN elimina la partición principal que incluye la información de formato del disco y las particiones lógicas del dispositivo.

Requisitos previos

Compruebe que ESXi no esté utilizando el dispositivo como disco de arranque, almacén de datos de VMFS o vSAN.

Procedimiento

1 Desplácese hasta el clúster de vSAN.

2 Haga clic en la pestaña **Configurar**.

3 En vSAN, haga clic en **Administración de discos**.

4 Seleccione un host para ver la lista de dispositivos disponibles.

5 En el menú desplegable **Mostrar**, seleccione **No válidos**.

6 Seleccione un dispositivo de la lista y haga clic en **Borrar particiones**.

7 Haga clic en **Aceptar** para confirmar.

   El dispositivo se encuentra limpio y no contiene información de particiones.

Aumentar la eficiencia de espacio en un clúster de vSAN

10

Puede utilizar las técnicas de eficiencia de espacio para reducir la cantidad de espacio para el almacenamiento de datos.

Estas técnicas reducen el espacio de almacenamiento total requerido para satisfacer sus necesidades.

Lea los siguientes temas a continuación:

Funciones de eficiencia de espacio de vSAN

Puede utilizar las técnicas de eficiencia de espacio para reducir la cantidad de espacio para el almacenamiento de datos.

Estas técnicas reducen la capacidad de almacenamiento total necesaria para satisfacer sus necesidades. vSAN 6.7 Update 1 y las versiones posteriores admiten comandos UNMPAP de SCSI que permiten reclamar espacio de almacenamiento asignado a un objeto de vSAN eliminado.

Puede usar la desduplicación y la compresión en un clúster de vSAN para eliminar los datos duplicados y reducir la cantidad de espacio necesario para almacenar datos. También puede utilizar vSAN de solo compresión para reducir los requisitos de almacenamiento sin comprometer el rendimiento del servidor.

Puede establecer el atributo de la directiva **Failure tolerance method** (Método de tolerancia ante errores) para utilizar la codificación de borrado RAID 5 o RAID 6. La codificación de borrado puede proteger sus datos y, al mismo tiempo, utilizar menos espacio de almacenamiento que el método de reflejo RAID 1 predeterminado.

Puede utilizar la desduplicación y compresión, y la codificación de borrado RAID 5 o RAID 6 para aumentar los ahorros en espacio de almacenamiento. RAID 5 o RAID 6 proporcionan ahorros de espacio claramente definidos en comparación con RAID 1. La desduplicación y la compresión pueden proporcionar ahorros adicionales.

Recuperar espacio de almacenamiento en vSAN con UNMAP de SCSI

Los comandos UNMAP de SCSI permiten recuperar espacio de almacenamiento que se asigna a archivos eliminados en el sistema de archivos creado por el invitado en el objeto de vSAN.

vSAN 6.7 Update 1 y versiones posteriores admiten UNMAP de SCSI. Al eliminar o quitar los archivos, se libera espacio en el sistema de archivos. Este espacio libre queda asignado a un dispositivo de almacenamiento hasta que el sistema de archivos lo libera o anula la asignación. vSAN admite la recuperación de espacio libre, también denominada operación de anulación de asignación. Puede liberar espacio de almacenamiento dentro del almacén de datos de vSAN al eliminar o migrar una máquina virtual o al consolidar una instantánea, entre otras acciones.

La recuperación de espacio de almacenamiento puede proporcionar una mayor capacidad de proceso de E/S de flash a host y mejorar la resistencia de flash.

La capacidad de anulación de asignación no está habilitada de forma predeterminada. Habilite **Recorte o anulación de asignación de invitados** en la pestaña de opciones avanzadas de los servicios de vSAN. Cuando habilite la anulación de asignación en un clúster de vSAN, deberá apagar y volver a encender todas las máquinas virtuales. Las máquinas virtuales deben usar hardware virtual versión 13 o posterior para poder realizar operaciones de anulación de asignación.

vSAN también admite los comandos UNMAP de SCSI emitidos directamente desde un sistema operativo invitado para recuperar espacio de almacenamiento. vSAN admite desasignaciones en línea y desasignaciones sin conexión. En el sistema operativo Linux, las anulaciones de asignación sin conexión se llevan a cabo con el comando **`fstrim(8)`**, y las anulaciones de asignación en línea se llevan a cabo cuando se utiliza el comando **`mount -o discard`**. En el sistema operativo Windows, NTFS lleva a cabo anulaciones de asignación en línea de forma predeterminada.

Usar la desduplicación y la compresión en un clúster de vSAN

vSAN puede realizar la desduplicación y compresión a nivel de bloque para ahorrar espacio de almacenamiento.

Cuando se habilitan la desduplicación y la compresión en un clúster basado en flash de vSAN, se reducen los datos redundantes dentro de cada grupo de discos o grupo de almacenamiento. La desduplicación elimina los bloques de datos redundantes, mientras que la compresión elimina los datos redundantes adicionales dentro de cada bloque de datos. Estas técnicas funcionan en conjunto para reducir la cantidad de espacio requerido para almacenar los datos. vSAN aplica la desduplicación y luego la compresión a medida que traslada los datos desde el nivel de memoria caché al nivel de capacidad. Use vSAN de solo compresión para cargas de trabajo que no se beneficien de la desduplicación, como el procesamiento transaccional en línea.

La desduplicación se produce en línea cuando los datos se vuelven a escribir desde el nivel de memoria caché al nivel de capacidad. El algoritmo de desduplicación utiliza un tamaño de bloque fijo y se aplica dentro de cada grupo de discos. Las copias redundantes de un bloque dentro del mismo grupo de discos se desduplican.

Para vSAN Original Storage Architecture, la desduplicación y la compresión se habilitan como una configuración para todo el clúster, pero se aplican a cada grupo de discos de forma individual. Además, no se puede habilitar la compresión en cargas de trabajo específicas, ya que la configuración no se puede cambiar a través de directivas de vSAN. Cuando habilite la desduplicación y compresión en un clúster de vSAN, se reducen los datos redundantes dentro de un grupo de discos en particular a una sola copia.

Nota Se aplicará vSAN de solo compresión en cada disco.

Para vSAN Express Storage Architecture, la compresión está habilitada de forma predeterminada en el clúster. Si no desea habilitar la compresión en algunas de las cargas de trabajo de la máquina virtual, puede hacerlo creando una directiva de almacenamiento personalizada y aplicando la directiva a las máquinas virtuales. Además, la compresión para vSAN Express Storage Architecture es solo para escrituras nuevas. Los bloques antiguos se dejan sin comprimir incluso después de activar la compresión de un objeto.

Puede habilitar la desduplicación y compresión cuando cree un clúster basado íntegramente en tecnología flash de vSAN o cuando edite un clúster basado íntegramente en tecnología flash de vSAN existente. Para obtener más información, consulte Habilitar la desduplicación y la compresión en un clúster de vSAN existente.

Cuando habilite o deshabilite la desduplicación y compresión, vSAN realizará un reformateo secuencial de cada grupo de discos o grupo de almacenamiento de cada host. De acuerdo con los datos almacenados en el almacén de datos de vSAN, este proceso podría demorar bastante tiempo. No realice estas operaciones con frecuencia. Si planifica deshabilitar la desduplicación y compresión, deberá verificar en primer lugar que exista suficiente capacidad física para colocar los datos.

Nota Puede que la desduplicación y la compresión no sean efectivas para las máquinas virtuales cifradas, ya que el cifrado de las máquinas virtuales cifra los datos del host antes de escribirlos fuera del almacenamiento. Tenga en cuenta los intercambios de almacenamiento cuando use el cifrado de máquinas virtuales.

Cómo administrar los discos en un clúster con desduplicación y compresión

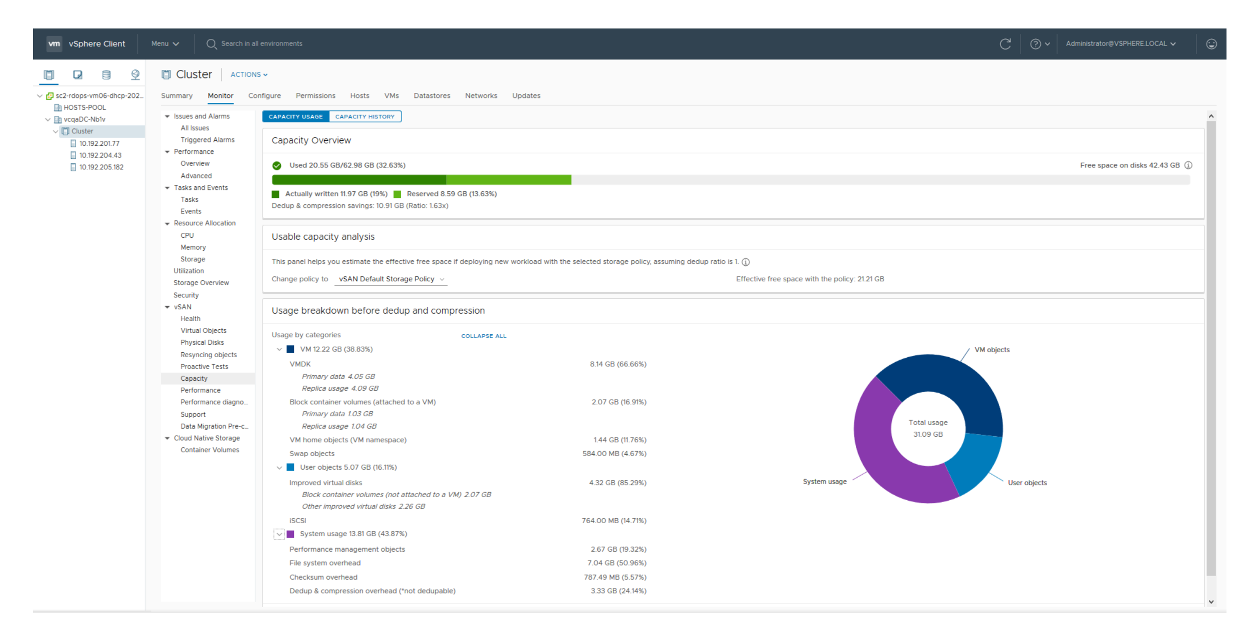
Nota Este tema solo se aplica a clústeres de vSAN Original Storage Architecture.

Considere las siguientes directrices al administrar discos en un clúster con la desduplicación y compresión habilitadas. Estas directrices no se aplican a vSAN de solo compresión.

- Evite agregar discos a un grupo de discos de forma incremental. Para lograr una desduplicación y una compresión más eficientes, considere agregar un grupo de discos para aumentar la capacidad de almacenamiento del clúster.
- Cuando incorpore un grupo de discos de forma manual, agregue todos los discos de capacidad al mismo tiempo.
- No es posible eliminar un solo disco de un grupo de discos. Deberá eliminar el grupo de discos entero para realizar modificaciones.
- El error de un solo disco provocará errores en el grupo de discos entero.

Cómo verificar los ahorros de espacio generados por la desduplicación y compresión

La cantidad de reducción de espacio generada por la desduplicación y compresión depende de varios factores, incluido el tipo de datos almacenados y la cantidad de bloques duplicados. Los grupos de discos más grandes tienden a brindar una proporción de desduplicación más elevada. Para comprobar los resultados de la desduplicación y la compresión, puede consultar el desglose del uso antes de la desduplicación y la compresión en el monitor de capacidad de vSAN.



Puede ver el desglose del uso antes de la desduplicación y la compresión cuando supervisa la capacidad de vSAN en vSphere Client. Muestra información sobre los resultados de la desduplicación y compresión. El espacio Usado antes indica el espacio lógico requerido antes de aplicar la desduplicación y compresión, mientras que el espacio Usado después indica el espacio físico usado después de aplicar la desduplicación y compresión. El espacio Usado después también muestra una descripción general de la cantidad de espacio ahorrado, y la proporción de la desduplicación y compresión.

La proporción de desduplicación y compresión se basa en el espacio Usado antes lógico requerido para almacenar los datos antes de la implementación de la desduplicación y compresión, en relación con el espacio Usado después físico requerido después de aplicar la desduplicación y compresión. Específicamente, la proporción es el espacio Usado antes dividido por el espacio Usado después. Por ejemplo, si el espacio Usado antes es 3 GB, pero el espacio Usado después físico es 1 GB, la proporción de desduplicación y compresión es 3x.

Cuando se habilitan la desduplicación y la compresión en el clúster de vSAN, es posible que las actualizaciones de capacidad demoren varios minutos en aparecer en Supervisión de capacidad, a medida que se va reclamando y reasignando el espacio de disco.

Consideraciones de diseño de desduplicación y compresión en un clúster de vSAN

Considere estas directrices al configurar la desduplicación y compresión en un clúster de vSAN.

- La desduplicación y compresión están disponibles solo en grupos de discos basados íntegramente en tecnología flash.
- Se requiere el formato en disco versión 3.0 o posterior para admitir la desduplicación y compresión.
- Deberá tener una licencia válida para poder habilitar la desduplicación y compresión en un clúster.
- Cuando habilite la desduplicación y compresión en un clúster de vSAN, todos los grupos de discos participarán en la reducción de datos a través de la desduplicación y compresión.
- vSAN puede eliminar los bloques de datos duplicados dentro de cada grupo de discos, pero no entre los grupos de discos (solo se aplica a vSAN Original Storage Architecture).
- La sobrecarga de capacidad para la desduplicación y compresión es aproximadamente un 5 % de la capacidad en bruto total.
- Las directivas deben tener reservas de espacio de objeto del 0 o del 100 %. Las directivas con reservas de espacio de objeto del 100 % siempre se respetan, pero pueden reducir la eficiencia de la desduplicación y la compresión.

Habilitar la desduplicación y la compresión en un nuevo clúster de vSAN

Puede habilitar la desduplicación y la compresión cuando se configura un nuevo clúster basado íntegramente en tecnología flash de vSAN.

Procedimiento

1. Desplácese hasta un nuevo clúster de vSAN basado en flash.
2. Haga clic en la pestaña **Configurar**.

3 En vSAN, seleccione **Servicios**.

   a Haga clic en **EDITAR** en **Servicios de datos**.

   b Seleccione una opción de eficiencia de espacio: Desduplicación y compresión, o Solo compresión.

   c En **Cifrado**, habilite el cifrado de datos en reposo usando el botón de alternancia.

   Nota Si utiliza el clúster vSAN Express Storage Architecture, no podrá cambiar esta configuración después de reclamar los discos.

   d (Opcional) Seleccione **Permitir redundancia reducida**. Si es necesario, vSAN reduce el nivel de protección de las máquinas virtuales mientras se habilitan la desduplicación y la compresión. Para obtener más información, consulte Reducir la redundancia de la máquina virtual para el clúster de vSAN.

4 Complete la configuración del clúster.

Habilitar la desduplicación y la compresión en un clúster de vSAN existente

Puede habilitar la desduplicación y la compresión mediante la edición de los parámetros de configuración de un clúster de vSAN basado en flash existente.

Para habilitar en un clúster de vSAN Original Storage Architecture:

1 Desplácese hasta el clúster de vSAN.

2 Haga clic en la pestaña **Configurar**.

3 En vSAN, seleccione **Servicios**.

   a Haga clic para editar la eficiencia de espacio.

   b Seleccione una opción de eficiencia de espacio: Desduplicación y compresión, o Solo compresión.

   c (Opcional) Seleccione **Permitir redundancia reducida**. Si es necesario, vSAN reduce el nivel de protección de las máquinas virtuales mientras se habilitan la desduplicación y la compresión. Para obtener más información, consulte Reducir la redundancia de la máquina virtual para el clúster de vSAN.

4 Haga clic en **Aplicar** para guardar los cambios realizados en la configuración.

Para habilitar en un clúster de vSAN Express Storage Architecture:

1 Desplácese hasta el clúster.

2 Haga clic en la pestaña **Configurar**.

3 En vSAN, seleccione **Servicios**.

4 En Servicios de datos, haga clic en **EDITAR**.

   a En **Cifrado**, habilite el cifrado de datos en reposo usando el botón de alternancia.

   Nota No podrá cambiar esta configuración después de reclamar los discos.

   b Habilite el cifrado de datos en tránsito usando el botón de alternancia Cifrado de datos en tránsito y especifique el intervalo de regeneración de claves.

   c (Opcional) Seleccione **Permitir redundancia reducida**. Si es necesario, vSAN reduce el nivel de protección de las máquinas virtuales mientras se habilitan la desduplicación y la compresión. Para obtener más información, consulte Reducir la redundancia de la máquina virtual para el clúster de vSAN.

5 Haga clic en **Aplicar** para guardar los cambios realizados en la configuración.

Mientras se habilitan la desduplicación y la compresión, vSAN actualiza el formato en disco de cada grupo de discos del clúster. Para llevar a cabo este cambio, vSAN evacua los datos del grupo de discos, quita el grupo de discos y lo vuelve a crear con un nuevo formato que admite desduplicación y compresión.

La operación de habilitación no requiere migración de máquinas virtuales ni DRS. El tiempo necesario para llevar a cabo esta operación depende de la cantidad de hosts del clúster y de la cantidad de datos. Puede supervisar el progreso en la pestaña **Tareas y eventos**.

Deshabilitar la desduplicación y la compresión en un clúster de vSAN

Puede deshabilitar la desduplicación y la compresión en el clúster de vSAN.

Cuando se deshabilitan la desduplicación y la compresión en el clúster de vSAN, se puede expandir el tamaño de la capacidad usada en el clúster (en función de la proporción de desduplicación). Antes de deshabilitar la desduplicación y la compresión, compruebe que el clúster tenga suficiente capacidad para gestionar el tamaño de los datos ampliados.

Procedimiento

1 Desplácese hasta el clúster de vSAN.

2 Haga clic en la pestaña **Configurar**.

   a En vSAN, seleccione **Servicios**.

   b Haga clic en **Editar**.

   c Deshabilite la desduplicación y la compresión.

   d (Opcional) Seleccione **Permitir redundancia reducida**. Si es necesario, vSAN reduce el nivel de protección de las máquinas virtuales a la vez que se deshabilitan la desduplicación y la compresión. Consulte Reducir la redundancia de la máquina virtual para el clúster de vSAN.

3 Haga clic en **Aplicar** o en **Aceptar** para guardar los cambios de configuración.

Resultados

Mientras se deshabilitan la desduplicación y la compresión, vSAN cambia el formato de disco de todos los grupos de discos del clúster. Evacua los datos del grupo de discos, quita el grupo de discos y lo vuelve a crear con un formato que no admite desduplicación y compresión.

El tiempo necesario para llevar a cabo esta operación depende de la cantidad de hosts del clúster y de la cantidad de datos. Puede supervisar el progreso en la pestaña **Tareas y eventos**.

Reducir la redundancia de la máquina virtual para el clúster de vSAN

Cuando se habilitan la desduplicación y la compresión, en algunos casos, puede que sea necesario reducir el nivel de protección de las máquinas virtuales.

Habilitar la desduplicación y la compresión requiere un cambio de formato de los grupos de discos. Para llevar a cabo este cambio, vSAN evacua los datos del grupo de discos, quita el grupo de discos y lo vuelve a crear con un nuevo formato que admite desduplicación y compresión.

En algunos entornos, puede que el clúster de vSAN no tenga suficientes recursos para evacuar por completo el grupo de discos. Un ejemplo de dicha implementación puede ser un clúster de tres nodos sin recursos para evacuar la réplica o el testigo manteniendo una protección completa. Otro ejemplo consiste en un clúster de cuatro nodos con objetos RAID-5 ya implementados. En el último caso, no habrá espacio para mover parte de la fracción RAID-5, ya que los objetos RAID-5 requieren un mínimo de cuatro nodos.

Aún así, se podrán habilitar la desduplicación y la compresión, y usar la opción Permitir redundancia reducida. Esta opción mantiene las máquinas virtuales en ejecución, pero puede que estas no sean capaces de tolerar el nivel total de errores definidos en la directiva de almacenamiento de máquina virtual. Por tanto, durante el cambio de formato para la desduplicación y la compresión, existiría el riesgo temporal de que las máquinas virtuales perdiesen datos. vSAN restaura la redundancia y el cumplimiento completos una vez finalizada la conversión de formato.

Agregar o quitar discos con desduplicación y compresión habilitadas

Cuando se agregan discos a un clúster de vSAN donde se han habilitado la desduplicación y la compresión, se aplican unas consideraciones específicas.

- Puede agregar un disco de capacidad a un grupo de discos con la desduplicación y la compresión habilitadas. No obstante, para una desduplicación y compresión más eficientes, en vez de agregar discos de capacidad, cree un grupo de discos para aumentar la capacidad de almacenamiento del clúster.
- Cuando se quita un discos de un nivel de memoria caché, se quita el grupo de discos completo. Si se quita un disco de nivel de memoria caché cuando la desduplicación y la compresión están habilitadas, se activa la evacuación de datos.

- La desduplicación y la compresión se implementan a nivel de grupo de discos. No puede quitar un disco de capacidad del clúster con la desduplicación y la compresión habilitadas. Debe quitar el grupo de discos completo.
- Si se produce un error en un disco de capacidad, no se podrá acceder a ninguno de los discos del grupo. Para solucionar este problema, identifique y sustituya el componente con errores inmediatamente. Al quitar el grupo de discos, use la opción Sin migración de datos.

Usar la codificación de borrado RAID 5 o RAID 6 en un clúster de vSAN

Puede utilizar la codificación de borrado RAID 5 o RAID 6 para ofrecer una protección frente a la pérdida de datos y aumentar la eficiencia del almacenamiento.

La codificación de borrado puede proporcionar el mismo nivel de protección de datos que el reflejo (RAID 1) y, al mismo tiempo, usar menos capacidad de almacenamiento. La codificación de borrado RAID 5 o RAID 6 permite que vSAN tolere los errores de hasta dos dispositivos de capacidad del almacén de datos. Puede configurar RAID 5 en clústeres basados íntegramente en tecnología flash con cuatro o más dominios de errores. Puede configurar RAID 5 o RAID 6 en clústeres basados íntegramente en tecnología flash con seis o más dominios de errores.

La codificación de borrado RAID 5 o RAID 6 requiere menos capacidad adicional para proteger los datos en comparación con el reflejo RAID 1. Por ejemplo, una máquina virtual protegida con un valor 1 en **Errores que se toleran** con RAID 1 requiere el doble del tamaño de disco virtual. Sin embargo, con RAID 5, se requiere 1,33 veces el tamaño de disco virtual. La siguiente tabla muestra una comparación general entre RAID 1 y RAID 5 o RAID 6.

Tabla 10-1. Capacidad requerida para almacenar y proteger los datos con diferentes niveles de RAID

Configuración de RAID	Errores que se toleran	Tamaño de los datos	Capacidad requerida
RAID 1 (creación de reflejos)	1	100 GB	200 GB
RAID 5 o RAID 6 (codificación de borrado) con cuatro dominios de errores	1	100 GB	133 GB
RAID 1 (creación de reflejos)	2	100 GB	300 GB
RAID 5 o RAID 6 (codificación de borrado) con seis dominios de errores	2	100 GB	150 GB

La codificación de borrado RAID 5 o RAID 6 es un atributo de directiva que puede aplicar a los componentes de las máquinas virtuales. Para utilizar RAID 5, establezca **Método de tolerancia a errores** en **RAID-5/6 (codificación de borrado)** y **Errores que se toleran** en 1. Para utilizar RAID 6, establezca **Método de tolerancia a errores** en **RAID-5/6 (codificación de borrado)** y **Errores que se toleran** en 2. La codificación de borrado RAID 5 o RAID 6 no admite un valor de 3 en **Errores que se toleran**.

Para utilizar RAID 1, establezca **Método de tolerancia a errores** en **RAID-1 (creación de reflejo)**. El reflejo RAID 1 requiere menos operaciones de E/S en los dispositivos de almacenamiento y, por lo tanto, puede proporcionar un mejor rendimiento. Por ejemplo, una resincronización del clúster demora menos tiempo en completarse con RAID 1.

Nota En un clúster ampliado de vSAN, el **Método de tolerancia a errores** de **RAID-5/6 (codificación de borrado)** se aplica únicamente a la opción **Tolerancia ante desastres de sitio**.

Nota Para un clúster de vSAN Express Storage Architecture, en función del número de dominios de errores que utilice, variará el número de componentes enumerados en **RAID 5** (**Supervisar** > **vSAN** > **Objetos virtuales** > testVM > **Ver los detalles de colocación**). Si hay seis o más dominios de errores disponibles en el clúster, se enumerarán cinco componentes en **RAID 5**. Si hay cinco o menos dominios de errores disponibles, se enumerarán tres componentes.

Para obtener más información sobre la configuración de las directivas, consulte Capítulo 7 Usar las directivas de vSAN.

Consideraciones de diseño de RAID 5 o RAID 6 en un clúster de vSAN

Considere estas directrices al configurar la codificación de borrado RAID 5 o RAID 6 en un clúster de vSAN.

- La codificación de borrado RAID 5 o RAID 6 está disponible solo en grupos de discos basados íntegramente en tecnología flash.
- Se requiere el formato en disco versión 3.0 o posterior para admitir RAID 5 o RAID 6.
- Deberá tener una licencia válida para poder habilitar RAID 5/6 en un clúster.
- Puede lograr ahorros de espacio adicionales al habilitar la desduplicación y la compresión en el clúster de vSAN.

Usar el cifrado en un clúster de vSAN

11

Puede cifrar los datos en tránsito de su clúster de vSAN y cifrar los datos en reposo de su almacén de datos de vSAN.

vSAN puede cifrar los datos en tránsito entre los hosts del clúster de vSAN. El cifrado de datos en tránsito protege los datos a medida que se mueven por el clúster de vSAN.

vSAN puede cifrar los datos en reposo del almacén de datos de vSAN. El cifrado de datos en reposo protege los datos de los dispositivos de almacenamiento, en caso de que un dispositivo se quite del clúster.

Lea los siguientes temas a continuación:

Cifrado de datos en tránsito de vSAN

vSAN puede cifrar los datos en tránsito mientras se mueve entre los hosts del clúster de vSAN.

vSAN puede cifrar los datos en tránsito entre los hosts del clúster. Cuando se habilita el cifrado de datos en tránsito, vSAN cifra todos los datos y el tráfico de metadatos entre los hosts.

El cifrado de datos en tránsito de vSAN tiene las siguientes características:

- vSAN utiliza el cifrado AES-256 bits en los datos en tránsito.
- El cifrado de datos en tránsito de vSAN no está relacionado con el cifrado de datos en reposo. Puede habilitar o deshabilitar cada uno por separado.
- Se aplica una confidencialidad directa al cifrado de datos en tránsito de vSAN.
- El tráfico entre los hosts de datos y los hosts testigo está cifrado.
- El tráfico de datos del servicio de archivos entre el proxy VDFS y el servidor VDFS está cifrado.
- Las conexiones entre hosts de los servicios de archivos de vSAN están cifradas.

vSAN utiliza claves simétricas que se generan de forma dinámica y se comparten entre hosts. Los hosts generan dinámicamente una clave de cifrado cuando establecen una transmisión, y utilizan la clave para cifrar todo el tráfico entre los hosts. No necesita un servidor de administración de claves para realizar el cifrado de datos en tránsito.

Cada host se autentica cuando se une al clúster, lo que garantiza que se permitan las conexiones únicamente a los hosts de confianza. Cuando se quita un host del clúster, se elimina el certificado de autenticación.

El cifrado de datos en tránsito de vSAN es una configuración que se aplica a todo el clúster. Si se habilita, todo el tráfico de datos y metadatos se cifrará en su tránsito por los hosts.

Habilitar el cifrado de datos en tránsito en un clúster de vSAN

Puede habilitar el cifrado de datos en tránsito mediante la edición de los parámetros de configuración de un clúster de vSAN.

Procedimiento

1 Desplácese hasta un clúster existente.

2 Haga clic en la pestaña **Configurar**.

3 En vSAN, seleccione **Servicios** y haga clic en el botón **Editar** de Cifrado de datos en tránsito.

4 Haga clic para habilitar el **Cifrado de datos en tránsito** y seleccione un intervalo de regeneración de claves.

5 Haga clic en **Aplicar**.

Resultados

Se habilitará el cifrado de datos en tránsito en el clúster de vSAN. vSAN cifra todos los datos que se mueven entre los hosts y las conexiones entre hosts del servicio de archivos en el clúster.

Cifrado de datos en reposo de vSAN

vSAN puede cifrar los datos en reposo del almacén de datos de vSAN.

Cuando habilite el cifrado de datos en reposo, vSAN cifrará los datos después de que se complete el resto de procesos, como la desduplicación. El cifrado de datos en reposo protege los datos de los dispositivos de almacenamiento, en caso de que un dispositivo se quite del clúster.

Para utilizar el cifrado en el almacén de datos de vSAN, se requiere algo de preparación. Una vez que el entorno está configurado, se puede habilitar el cifrado de los datos en reposo en el clúster de vSAN.

El cifrado de datos en reposo requiere un servidor de administración de claves (KMS) externo o un vSphere Native Key Provider. Para obtener más información sobre el cifrado de vSphere, consulte *Seguridad de vSphere*.

Puede utilizar un servidor de administración de claves (KMS) externo, el sistema vCenter Server y sus hosts ESXi para cifrar los datos en su clúster vSAN. vCenter Server solicita claves de cifrado desde un KMS externo. El KMS genera y almacena las claves, y vCenter Server obtiene los identificadores de claves del KMS y los distribuye en los hosts ESXi.

vCenter Server no almacena las claves del KMS, pero sí conserva una lista de identificadores de claves.

Cómo funciona el cifrado de datos en reposo de vSAN

Cuando se habilita el cifrado de datos en reposo, vSAN cifra todo el contenido del almacén de datos de vSAN.

Como se cifra la totalidad de los archivos, todas las máquinas virtuales y sus correspondientes datos quedan protegidos. Solo los administradores con privilegios de cifrado pueden realizar tareas de cifrado y descifrado. vSAN utiliza las claves de cifrado de la siguiente manera:

- vCenter Server solicita a KMS una clave de cifrado de claves (Key Encryption Key, KEK) AES-256. vCenter Server almacena solo el identificador de la KEK, pero no la clave en sí.
- El host ESXi cifra los datos del disco mediante el modo AES-256 XTS estándar del sector. Cada disco tiene una clave de cifrado de datos (Data Encryption Key, DEK) diferente que se genera al azar.
- Cada host ESXi usa la KEK para cifrar sus DEK y almacena las DEK cifradas en el disco. El host no almacena la KEK en el disco. Si un host se reinicia, solicita a KMS la KEK con el identificador correspondiente. A continuación, el host puede descifrar sus DEK según lo necesite.
- La clave de un host no se usa para cifrar datos, sino volcados de núcleos. Todos los hosts de un mismo clúster usan la misma clave de host. Al recopilar paquetes de soporte, se genera una clave al azar para volver a cifrar los volcados de núcleo. Puede especificar una contraseña para cifrar la clave aleatoriamente.

Cuando un host se reinicia, no monta sus grupos de discos hasta recibir la KEK. Este proceso puede tardar varios minutos o más en completarse. Es posible supervisar el estado de los grupos de discos en vSAN Health Service, en **Discos físicos > Estado de software**.

Persistencia de claves de cifrado

En vSAN 7.0 Update 3 y versiones posteriores, el cifrado de datos en reposo puede seguir funcionando incluso cuando el servidor de claves está temporalmente sin conexión o no disponible. Con la persistencia de claves habilitada, los hosts ESXi pueden conservar las claves de cifrado incluso después de un reinicio.

Cada host ESXi obtiene las claves de cifrado al inicio y las conserva en su memoria caché de claves. Si el host ESXi tiene un módulo de plataforma de confianza (TPM), las claves de cifrado se conservan en el TPM después de reiniciar. El host no necesita solicitar claves de cifrado. Las operaciones de cifrado pueden continuar cuando el servidor de claves no está disponible, ya que las claves han persistido en el TPM.

Utilice los siguientes comandos para habilitar la persistencia de claves en un host de clúster.

```
esxcli system settings encryption set --mode=TPM
```

```
esxcli system security keypersistence enable
```

Para obtener más información sobre la persistencia de claves de cifrado, consulte "Descripción general de la persistencia de claves" en *Seguridad de vSphere*.

Usar vSphere Native Key Provider

vSAN 7.0 Update 2 admite vSphere Native Key Provider. Si el entorno está configurado para vSphere Native Key Provider, puede usarlo para cifrar las máquinas virtuales de su clúster de vSAN. Para obtener más información, consulte "Configurar y administrar vSphere Native Key Provider" en *Seguridad de vSphere*.

vSphere Native Key Provider no requiere un servidor de administración de claves (KMS) externo. vCenter Server genera la clave de cifrado de claves y la aplica a los hosts ESXi. A continuación, los hosts ESXi generan claves de cifrado de datos.

Nota Si utiliza vSphere Native Key Provider, asegúrese de hacer una copia de seguridad del proveedor de claves nativo para garantizar que las tareas de reconfiguración se ejecuten sin problemas.

vSphere Native Key Provider puede coexistir con una infraestructura de servidor de claves ya existente.

Consideraciones de diseño para el cifrado de datos en reposo de vSAN

Tenga en cuenta las siguientes directrices al trabajar con el cifrado de datos en reposo.

- No implemente el servidor KMS en el mismo almacén de datos de vSAN que planea cifrar.
- El cifrado requiere gran consumo de CPU. AES-NI mejora ampliamente el rendimiento de cifrado. Habilite AES-NI en el BIOS.
- El host testigo de un clúster ampliado de vSAN no participa en el cifrado de vSAN. El host testigo no almacena datos del cliente, solo metadatos, como el tamaño y el UUID de objetos y componentes de vSAN.

  Nota Si el host testigo es un dispositivo que se ejecuta en otro clúster, puede cifrar los metadatos almacenados en él. Habilite el cifrado de datos en reposo en el clúster que contiene el host testigo.

- Establezca una directiva para los volcados de núcleo. Los volcados de núcleo se cifran debido a que pueden contener información confidencial. Al descifrar un volcado de núcleo, maneje la información confidencial con cuidado. Los volcados de núcleo de ESXi pueden contener claves para el host ESXi y para los datos que este contiene.
  - Siempre utilice una contraseña para recopilar un paquete de `vm-support`. Puede especificar la contraseña al generar el paquete de soporte desde vSphere Client o puede utilizar el comando `vm-support`.

    La contraseña vuelve a cifrar los volcados de núcleo que utilizan claves internas de manera que estos volcados empleen claves basadas en la contraseña. Posteriormente, se puede usar la contraseña para descifrar cualquier volcado de núcleo cifrado que pudiera estar incluido en el paquete de soporte. Esto no afecta a los volcados de núcleo ni a los registros sin cifrar.
  - La contraseña que especificó durante la creación del paquete de `vm-support` no persiste en los componentes de vSphere. Es su responsabilidad llevar un registro de las contraseñas de los paquetes de soporte.

Configurar el proveedor de claves estándar

Use un proveedor de claves estándar para distribuir las claves que cifran el almacén de datos de vSAN.

Antes de poder cifrar el almacén de datos de vSAN, debe configurar un proveedor de claves estándar para admitir el cifrado. Esa tarea incluye agregar el KMS a vCenter Server y establecer confianza con el KMS. vCenter Server proporciona claves de cifrado desde el proveedor de claves.

KMS debe ser compatible con el protocolo estándar de interoperabilidad de administración de claves (KMIP) 1.1. Consulte más información en *Matrices de compatibilidad de vSphere*.

Agregar un KMS a vCenter Server

Los servidores de administración de claves (KMS) se agregan a los sistemas vCenter Server desde vSphere Client.

vCenter Server crea un proveedor de claves estándar cuando se agrega la primera instancia de KMS. Si configura el proveedor de claves en dos o más instancias de vCenter Server, asegúrese de que utiliza el mismo nombre de proveedor de claves.

Nota No implemente los servidores KMS en el clúster de vSAN que planea cifrar. Si se produce un error, los hosts del clúster de vSAN deberán comunicarse con el servidor KMS.

- Al agregar el servidor KMS, se solicitará establecer este proveedor de claves como predeterminado. Más adelante podrá cambiar la configuración predeterminada.
- Una vez que vCenter Server crea el primer proveedor de claves, podrá agregar instancias de KMS del mismo proveedor de claves y configurar todas las instancias de KMS para sincronizar las claves entre ellos. Utilice el método documentado por el proveedor de KMS.

- Puede configurar el proveedor de claves con una sola instancia de KMS.
- Si el entorno admite soluciones de KMS de diferentes proveedores, podrá agregar varios proveedores de claves.

Requisitos previos

- Compruebe que el servidor de administración de claves se encuentre en *Matrices de compatibilidad de vSphere* y que cumpla con KMIP 1.1.
- Compruebe que dispone de los privilegios necesarios: **Cryptographer.ManageKeyServers (Criptógrafo.AdministrarServidoresClaves).**
- No se admite la conexión con un KMS exclusivamente por medio de una dirección IPv6.
- No se admite la conexión con un KMS a través de un servidor proxy que requiera nombre de usuario o contraseña.

Procedimiento

1 Inicie sesión en vCenter Server.

2 Examine la lista de inventario y seleccione la instancia de vCenter Server.

3 Haga clic en **Configurar** y, en Seguridad, haga clic en **Proveedores de claves**.

4 Haga clic en **Agregar proveedor de claves estándar**, introduzca la información del proveedor de claves y haga clic en **Agregar proveedor de claves**.

  Puede hacer clic en **Agregar KMS** para agregar más servidores de administración de claves.

5 Haga clic en **Confianza**.

  vCenter Server agregará el proveedor de claves y mostrará el estado como Conectado.

Establecer una conexión de confianza de proveedor de claves estándar mediante el intercambio de certificados

Después de agregar el proveedor de claves estándar al sistema vCenter Server, puede establecer una conexión de confianza.

El proceso exacto depende de los certificados que el proveedor de claves acepte y de la directiva de su empresa.

Requisitos previos

Agregue el proveedor de claves estándar.

Procedimiento

1 Desplácese hasta vCenter Server.

2 Haga clic en **Configurar** y seleccione **Proveedores de claves** en **Seguridad**.

3 Seleccione el proveedor de claves.

  Se muestra el KMS para el proveedor de claves.

4 Seleccione el KMS.

5 En el menú desplegable **Establecer confianza**, seleccione **Hacer que KMS confíe en vCenter**.

6 Seleccione la opción adecuada para el servidor y complete los pasos.

Opción	Consulte
Certificado de CA raíz de vCenter Server	Usar la opción Certificado de CA raíz para establecer una conexión de confianza con el proveedor de claves estándar.
Certificado de vCenter Server	Usar la opción Certificado para establecer una conexión de confianza con el proveedor de claves estándar.
Cargar certificado y clave privada	Usar la opción Cargar certificado y clave privada para establecer una conexión de confianza con el proveedor de claves estándar.
Nueva solicitud de firma de certificado	Usar la opción Nueva solicitud de firma de certificado para establecer una conexión de confianza con el proveedor de claves estándar.

Usar la opción Certificado de CA raíz para establecer una conexión de confianza con el proveedor de claves estándar

Algunos proveedores de KMS requieren que se cargue el certificado de CA raíz al KMS.

Este KMS establece una conexión de confianza con todos los certificados firmados por la entidad de certificación de raíz. El certificado de CA raíz que utiliza el cifrado de máquinas virtuales de vSphere es un certificado autofirmado que se almacena en un almacén separado en VMware Endpoint Certificate Store (VECS) en el sistema de vCenter Server.

Nota Genere un certificado de CA raíz solo si desea reemplazar los certificados existentes. En ese caso, los demás certificados que están firmados por esa entidad de certificación raíz dejan de ser válidos. Se puede generar un nuevo certificado de CA raíz como parte de este flujo de trabajo.

Procedimiento

1 Desplácese hasta vCenter Server.

2 Haga clic en **Configurar** y seleccione **Proveedores de claves** en **Seguridad**.

3 Seleccione el proveedor de claves con el cual desea establecer una conexión de confianza.

Se muestra el KMS para el proveedor de claves.

4 En el menú desplegable **Establecer confianza**, seleccione **Hacer que KMS confíe en vCenter**.

5 Seleccione **Certificado de CA raíz de vCenter** y haga clic en **Siguiente**.

El cuadro de diálogo Descargar certificado de CA raíz se rellena con el certificado raíz que vCenter Server utiliza para el cifrado. Este certificado se almacena en el almacén VECS.

6 Copie el certificado en el portapapeles o descárguelo como un archivo.

7 Siga las instrucciones de su proveedor de KMS para cargar el certificado al sistema.

Nota Algunos proveedores de KMS requieren que el proveedor de KMS reinicie el KMS para seleccionar el certificado raíz que se cargó.

Pasos siguientes

Finalice el intercambio de certificados. Consulte Finalizar la configuración de confianza de un proveedor de claves estándar.

Usar la opción Certificado para establecer una conexión de confianza con el proveedor de claves estándar

Algunos proveedores de KMS requieren que se cargue el certificado de vCenter Server al KMS.

Después de la carga, el KMS acepta el tráfico proveniente de un sistema con ese certificado. vCenter Server genera un certificado para proteger las conexiones con el KMS. El certificado se almacena en un almacén de claves separado en VMware Endpoint Certificate Store (VECS) en el sistema de vCenter Server.

Procedimiento

1 Desplácese hasta vCenter Server.

2 Haga clic en **Configurar** y seleccione **Proveedores de claves** en **Seguridad**.

3 Seleccione el proveedor de claves con el cual desea establecer una conexión de confianza.

Se muestra el KMS para el proveedor de claves.

4 En el menú desplegable **Establecer confianza**, seleccione **Hacer que KMS confíe en vCenter**.

5 Seleccione **Certificado de vCenter** y haga clic en **Siguiente**.

El cuadro de diálogo Download Certificate (Descargar certificado) se rellena con el certificado raíz que vCenter Server utiliza para el cifrado. Este certificado se almacena en el almacén VECS.

Nota No genere un certificado nuevo a menos que desee reemplazar los certificados existentes.

6 Copie el certificado en el portapapeles o descárguelo como un archivo.

7 Siga las instrucciones de su proveedor de KMS para cargar el certificado al KMS.

Pasos siguientes

Finalice la relación de confianza. Consulte Finalizar la configuración de confianza de un proveedor de claves estándar.

Usar la opción Nueva solicitud de firma de certificado para establecer una conexión de confianza con el proveedor de claves estándar

Algunos proveedores de KMS requieren que vCenter Server genere una solicitud de firma del certificado (Certificate Signing Request, CSR) y la envíe al KMS.

El KMS firma la CSR y devuelve el certificado firmado. El certificado firmado se puede cargar en vCenter Server. El uso de la opción **Nueva solicitud de firma de certificado** es un proceso de dos pasos. Primero debe generar la CSR y enviarla al proveedor de KMS. A continuación, cargue el certificado firmado que recibió del proveedor de KMS a vCenter Server.

Procedimiento

1 Desplácese hasta vCenter Server.

2 Haga clic en **Configurar** y seleccione **Proveedores de claves** en **Seguridad**.

3 Seleccione el proveedor de claves con el cual desea establecer una conexión de confianza.

Se muestra el KMS para el proveedor de claves.

4 En el menú desplegable **Establecer confianza**, seleccione **Hacer que KMS confíe en vCenter**.

5 Seleccione **Nueva solicitud de firma de certificado (CSR)** y haga clic en **Siguiente**.

6 En el cuadro de diálogo, copie el certificado completo del cuadro de texto en el portapapeles o descárguelo como un archivo.

Use el botón **Generar nueva CSR** del cuadro de diálogo únicamente si desea generar una CSR de forma explícita.

7 Siga las instrucciones de su proveedor de KMS para enviar la CSR.

8 Cuando reciba el certificado firmado del proveedor de KMS, vuelva a hacer clic en **Proveedores de claves**, seleccione el proveedor de claves y, en el menú desplegable **Establecer confianza**, seleccione **Cargar certificado de CSR firmado**.

9 Pegue el certificado firmado en el cuadro de texto inferior o haga clic en **Cargar archivo** y cargue el archivo; luego, haga clic en **Aceptar**.

Pasos siguientes

Finalice la relación de confianza. Consulte Finalizar la configuración de confianza de un proveedor de claves estándar.

Usar la opción Cargar certificado y clave privada para establecer una conexión de confianza con el proveedor de claves estándar

Algunos proveedores de KMS requieren que se carguen el certificado del servidor KMS y la clave privada al sistema de vCenter Server.

Algunos proveedores de KMS generan un certificado y una clave privada para la conexión y los vuelven disponibles para el usuario. Una vez que haya cargado los archivos, el KMS establecerá una conexión de confianza con su instancia de vCenter Server.

Requisitos previos

- Solicite un certificado y una clave privada al proveedor de KMS. Los archivos son archivos X509 en formato PEM.

Procedimiento

1 Desplácese hasta vCenter Server.

2 Haga clic en **Configurar** y seleccione **Proveedores de claves** en **Seguridad**.

3 Seleccione el proveedor de claves con el cual desea establecer una conexión de confianza.

   Se muestra el KMS para el proveedor de claves.

4 En el menú desplegable **Establecer confianza**, seleccione **Hacer que KMS confíe en vCenter**.

5 Seleccione **Certificado y clave privada de KMS** y haga clic en **Siguiente**.

6 Pegue el certificado que recibió del proveedor de KMS en el cuadro de texto superior o haga clic en **Cargar un archivo** para cargar el archivo del certificado.

7 Pegue el archivo de claves en el cuadro de texto inferior o haga clic en **Cargar un archivo** para cargar el archivo de claves.

8 Haga clic en **Establecer confianza**.

Pasos siguientes

Finalice la relación de confianza. Consulte Finalizar la configuración de confianza de un proveedor de claves estándar.

Establecer el proveedor de claves predeterminado mediante vSphere Client

Puede utilizar vSphere Client para establecer el proveedor de claves predeterminado en el nivel de vCenter Server.

Debe establecer el proveedor de claves predeterminado si no establece el primer proveedor de claves como predeterminado o si el entorno usa varios proveedores de claves y se elimina el predeterminado.

Requisitos previos

Como práctica recomendada, compruebe que el estado de conexión en la pestaña Proveedores de claves sea Activo y tenga una marca de verificación verde.

Procedimiento

1 Inicie sesión en vSphere Client.

2 Desplácese hasta vCenter Server.

3 Haga clic en **Configurar** y seleccione **Proveedores de claves** en **Seguridad**.

4 Seleccione el proveedor de claves.

5 Haga clic en **Establecer como valor predeterminado**.

   Se mostrará un cuadro de diálogo de confirmación.

6 Haga clic en **Establecer como valor predeterminado**.

   El proveedor de claves se muestra como la selección predeterminada actual.

Finalizar la configuración de confianza de un proveedor de claves estándar

A menos que el cuadro de diálogo **Agregar proveedor de claves estándar** le solicite confiar en el KMS, debe establecer la confianza explícitamente una vez finalizado el intercambio de certificados.

Es posible completar la instalación de confianza, es decir, hacer que vCenter Server confíe en el KMS, ya sea confiando en el KMS o cargando un certificado de KMS. Tiene dos opciones:

- Confiar en el certificado explícitamente por medio de la opción **Cargar certificado de KMS**.
- Cargar un certificado de hoja de KMS o el certificado de CA de KMS en vCenter Server por medio de la opción **Hacer que vCenter confíe en KMS**.

Nota Si carga el certificado de CA raíz o el certificado de CA intermedia, vCenter Server confía en todos los certificados que firma esa CA. Si desea obtener una seguridad más solida, cargue un certificado de hoja o un certificado de CA intermedia que controle el proveedor de KMS.

Procedimiento

1 Desplácese hasta vCenter Server.

2 Haga clic en **Configurar** y seleccione **Proveedores de claves** en **Seguridad**.

3 Seleccione el proveedor de claves con el cual desea establecer una conexión de confianza.

Se muestra el KMS para el proveedor de claves.

4 Seleccione el KMS.

5 Seleccione una de las siguientes opciones en el menú desplegable **Establecer confianza**.

Opción	Acción
Hacer que vCenter confíe en KMS	En el cuadro de diálogo que aparece, haga clic en **Confiar**.
Cargar certificado de KMS	a En el cuadro de diálogo que aparece, pegue el certificado o haga clic en **Cargar un archivo** y desplácese hasta el archivo de certificado. b Haga clic en **Cargar**.

Habilitar el cifrado de datos en reposo en un clúster de vSAN nuevo

Puede habilitar el cifrado de datos en reposo cuando se configura un nuevo clúster de vSAN.

Requisitos previos

- Privilegios necesarios:
  - **Host.Inventory.EditCluster** (Host.Inventario.EditarClúster)
  - **Cryptographer.ManageEncryptionPolicy**(Criptógrafo.AdministrarDirectivaCifrado)
  - **Cryptographer.ManageKMS**(Criptógrafo.AdministrarKMS)
  - **Cryptographer.ManageKeys**(Criptógrafo.AdministrarClaves)

- Debe haber configurado un proveedor de claves estándar y establecido una conexión de confianza entre vCenter Server y el KMS.

Procedimiento

1 Desplácese hasta un clúster existente.
2 Haga clic en la pestaña **Configurar**.
3 En vSAN, seleccione **Servicios** y haga clic en el botón **Editar** de Cifrado.
4 En el cuadro de diálogo **Servicios de vSAN**, habilite el **Cifrado** y seleccione un clúster de KMS o un proveedor de claves.

    Nota Marque la casilla de verificación **Eliminar datos residuales** para borrar los datos residuales de los dispositivos antes de habilitar el cifrado de vSAN. Asegúrese de anular la selección de esta casilla de verificación, a menos que desee eliminar los datos existentes de los dispositivos de almacenamiento al cifrar un clúster que contenga datos de la máquina virtual. De esta manera, se garantiza que los datos sin cifrar ya no se encuentren en los dispositivos después de habilitar el cifrado vSAN. Esta opción no es necesaria para instalaciones nuevas que no tengan datos de máquinas virtuales en los dispositivos de almacenamiento.

5 Complete la configuración del clúster.

Resultados

En el clúster de vSAN, se habilita el cifrado de datos en reposo. vSAN cifra todos los datos que se agregan al almacén de datos de vSAN.

Generar nuevas claves de cifrado de datos en reposo

Es posible crear nuevas claves de cifrado de datos en reposo en caso de que una clave caduque o se vea comprometida.

Al generar nuevas claves de cifrado para el clúster de vSAN, están disponibles las siguientes opciones:

- Si genera una nueva KEK, todos los hosts del clúster de vSAN reciben la nueva KEK del KMS. La DEK de cada host se vuelve a cifrar con la nueva KEK.
- Si elige realizar una regeneración de claves profunda y volver a cifrar todos los datos con claves nuevas, se generan una nueva KEK y una nueva DEK. Para volver a cifrar los datos, es preciso reformatear el disco en forma sucesiva.

Requisitos previos

- Privilegios necesarios:
  - **Host.Inventory.EditCluster** (Host.Inventario.EditarClúster)
  - **Cryptographer.ManageKeys**(Criptógrafo.AdministrarClaves)

- Se debe haber configurado un proveedor de claves y establecido una conexión de confianza entre vCenter Server y KMS.

Procedimiento

1 Desplácese hasta el clúster de hosts de vSAN.
2 Haga clic en la pestaña **Configurar**.
3 En vSAN, seleccione **Servicios**.
4 Haga clic en **Generar nuevas claves de cifrado**.
5 Para generar una nueva KEK, haga clic en **Aplicar**. Las DEK se volverán a cifrar con la nueva KEK.
   - Para generar una nueva KEK y nuevas DEK, y para volver a cifrar todos los datos del clúster de vSAN, active la siguiente casilla: **También vuelva a cifrar todos los datos en el almacenamiento con nuevas claves**.
   - Si el clúster de vSAN tiene recursos limitados, marque la casilla **Permitir redundancia reducida**. Si permite la redundancia reducida, es posible que los datos estén en riesgo durante la operación de reformateo de disco.

Habilitar el cifrado de datos en reposo en un clúster de vSAN existente

Puede habilitar el cifrado de datos en reposo en los clústeres de vSAN OSA y vSAN ESA existentes.

Requisitos previos

- Privilegios necesarios:
  - **Host.Inventory.EditCluster** (Host.Inventario.EditarClúster)
  - **Cryptographer.ManageEncryptionPolicy**(Criptógrafo.AdministrarDirectivaCifrado)
  - **Cryptographer.ManageKMS**(Criptógrafo.AdministrarKMS)
  - **Cryptographer.ManageKeys**(Criptógrafo.AdministrarClaves)
- Debe haber configurado un proveedor de claves estándar y establecido una conexión de confianza entre vCenter Server y el KMS.
- El reclamo de discos del clúster debe estar configurado en modo manual.

Procedimiento

1 Desplácese hasta el clúster de hosts de vSAN.
2 Haga clic en la pestaña **Configurar**.
3 En vSAN, seleccione **Servicios**.
4 Haga clic en el botón **Editar cifrado**.

5 En el cuadro de diálogo Servicios de vSAN, habilite el **Cifrado** y seleccione un clúster de KMS o un proveedor de claves.

6 (Opcional) Si los dispositivos de almacenamiento del clúster contienen datos confidenciales, seleccione **Eliminar datos residuales**.

   Con esta configuración, vSAN borra los datos existentes de los dispositivos de almacenamiento durante el cifrado. Esta opción puede aumentar el tiempo para procesar cada disco, así que no la seleccione a menos que tenga datos no deseados en los discos.

7 Haga clic en **Aplicar**.

Resultados

Se lleva a cabo un reformateo sucesivo de todos los grupos de discos mientras vSAN cifra todos los datos en el almacén de datos de vSAN.

Pasos siguientes

Puede desactivar el cifrado en el clúster en cualquier momento. Será necesario reformatear el disco, ya que vSAN descifra todos los datos del almacén de datos.

Cifrado y volcados de núcleo en vSAN

Si el clúster de vSAN utiliza cifrado de datos en reposo y si se produce un error en el host ESXi, el volcado de núcleo resultante se cifra para proteger los datos.

Los volcados de núcleo que se incluyen en el paquete de `vm-support` también están cifrados.

Nota Los volcados de núcleo pueden contener información confidencial. Siga la directiva de seguridad de datos y privacidad de la organización al gestionar el volcado de núcleo.

Volcados de núcleo en hosts ESXi

Cuando un host ESXi se bloquea, se genera un volcado de núcleo cifrado y el host se reinicia. El volcado de núcleo se cifra con la clave de host que se encuentra en la memoria caché de claves de ESXi. Lo que puede hacer a continuación depende de diversos factores.

- En la mayoría de los casos, vCenter Server recupera la clave del host del KMS e intenta insertar la clave en el host ESXi después de reiniciar. Si la operación se realiza correctamente, se puede generar el paquete de `vm-support` y descifrar o volver a cifrar el volcado de núcleo.
- Si vCenter Server no puede conectarse al host ESXi, tal vez se pueda recuperar la clave del KMS.
- Si el host usó una clave personalizada que no es igual a la clave que vCenter Server inserta en el host, no se podrá manipular el volcado de núcleo. Evite usar claves personalizadas.

Volcados de núcleo y paquetes de vm-support

Si se comunica con el soporte técnico de VMware debido a un error grave, el representante de soporte, por lo general, le pedirá que genere un paquete de `vm-support`. El paquete incluye archivos de registro y otra información, incluso volcados de núcleo. Si los representantes de soporte no pueden resolver los inconvenientes al analizar los archivos de registro y otra información, el usuario puede descifrar los volcados de núcleo para habilitar la información relevante. Siga la directiva de seguridad y privacidad de la organización para proteger la información confidencial, como las claves de host.

Volcados de núcleo de sistemas vCenter Server

Un volcado de núcleo de un sistema vCenter Server no está cifrado. vCenter Server ya contiene información posiblemente confidencial. Como mínimo, asegúrese de que vCenter Server esté protegido. Asimismo, también se recomienda apagar los volcados de núcleo del sistema de vCenter Server. Otra información de los archivos de registro puede ayudar a determinar el problema.

Recopilar un paquete de vm-support para un host de ESXi en un almacén de datos de vSAN cifrado

Cuando se habilita el cifrado de datos en reposo en un clúster de vSAN, se cifran todos los volcados de núcleo en el paquete de `vm-support`.

Puede recopilar el paquete y especificar una contraseña si piensa descifrar el volcado de núcleo más adelante. El paquete de `vm-support` incluye archivos de registro y archivos de volcado de núcleo, entre otros.

Requisitos previos

Notifique a su representante de soporte que se habilitó el cifrado de datos en reposo para el almacén de datos de vSAN. Es posible que el representante le pida descifrar los volcados de núcleo para extraer información relevante.

Nota Los volcados de núcleo pueden contener información confidencial. Siga la directiva de seguridad y privacidad de la organización para proteger la información confidencial, como las claves de host.

Procedimiento

1. Inicie sesión en vCenter Server mediante vSphere Client.
2. Haga clic en **Hosts and Clusters** (Hosts y clústeres) y, a continuación, haga clic con el botón derecho en el host ESXi.
3. Seleccione **Export System Logs** (Exportar registros del sistema).
4. En el cuadro de diálogo, seleccione **Password for encrypted core dumps** (Contraseña para volcados de núcleo cifrados) y, a continuación, especifique y confirme una contraseña.

5 Deje los valores predeterminados para las otras opciones o realice cambios si así lo requiere el soporte técnico de VMware, y haga clic en **Finish** (Finalizar).

6 Especifique una ubicación para el archivo.

7 Si su representante de soporte le pidió descifrar el volcado de núcleo en el paquete de `vm-support`, inicie sesión en cualquier host ESXi y siga estos pasos.

   a Inicie sesión en ESXi y conéctese al directorio donde se encuentra el paquete de `vm-support`.

   El nombre de archivo sigue el patrón **`esx.fecha_y_hora.tgz`**.

   b Asegúrese de que el directorio tenga suficiente espacio para el paquete, el paquete descomprimido y el paquete nuevamente comprimido, o mueva el paquete.

   c Extraiga el paquete en el directorio local.

   ```
   vm-support -x *.tgz .
   ```

   La jerarquía de archivos resultante puede contener los archivos de volcado de núcleo para el host ESXi, generalmente en `/var/core`, y puede contener varios archivos de volcado de núcleo de las máquinas virtuales.

   d Descifre cada archivo de volcado de núcleo cifrado por separado.

   ```
   crypto-util envelope extract --offset 4096 --keyfile vm-support-incident-key-file
   --password encryptedZdump decryptedZdump
   ```

   vm-support-incident-key-file es el archivo de claves de incidentes que se encuentra en el nivel superior del directorio.

   encryptedZdump es el nombre del archivo de volcado de núcleo cifrado.

   decryptedZdump es el nombre del archivo que genera el comando. Procure que el nombre sea similar al nombre de *encryptedZdump*.

   e Proporcione la contraseña que especificó al crear el paquete de `vm-support`.

   f Elimine los volcados de núcleo cifrados y vuelva a comprimir el paquete.

   ```
   vm-support --reconstruct
   ```

8 Elimine los archivos que contengan información confidencial.

Descifrar o volver a cifrar un volcado de núcleo cifrado en un host ESXi

Para descifrar o volver a cifrar un volcado de núcleo cifrado en el host ESXi, se puede usar la CLI `crypto-util`.

Puede descifrar y examinar por su cuenta los volcados de núcleo en el paquete de `vm-support`. Los volcados de núcleo pueden contener información confidencial. Siga la directiva de seguridad y privacidad de la organización para proteger la información confidencial, como las claves de host.

Para obtener detalles sobre la forma de volver a cifrar un volcado de núcleo y usar otras funciones de `crypto-util`, consulte la ayuda de la línea de comandos.

Nota `crypto-util` es para usuarios avanzados.

Requisitos previos

La clave de host ESXi que se usó para cifrar el volcado de núcleo debe estar disponible en el host ESXi que generó el volcado de núcleo.

Procedimiento

1 Inicie sesión directamente en el host ESXi donde se produjo el volcado de núcleo.

Si el host ESXi se encuentra en el modo de bloqueo, o si el acceso SSH no está habilitado, es posible que primero deba habilitar el acceso.

2 Determine si el volcado de núcleo está cifrado.

Opción	Descripción
Supervisar el volcado de núcleo	`crypto-util envelope describe vmmcores.ve`
archivo zdump	`crypto-util envelope describe --offset 4096` *`zdumpFile`*

3 Descifre el volcado de núcleo según su tipo.

Opción	Descripción
Supervisar el volcado de núcleo	`crypto-util envelope extract vmmcores.ve vmmcores`
archivo zdump	`crypto-util envelope extract --offset 4096` *`zdumpEncrypted zdumpUnencrypted`*

Actualizar el clúster de vSAN

12

La actualización de vSAN es un proceso de varias etapas, en el cual los procedimientos de actualización se deben llevar a cabo en el orden que se describe aquí.

Nota No se puede actualizar un clúster de vSAN Original Storage Architecture a vSAN Express Storage Architecture mediante vSphere Client o Ruby vSphere Console (RVC).

Antes de intentar realizar la actualización, asegúrese de comprender claramente todo el proceso de actualización, a fin de garantizar una actualización correcta y sin interrupciones. Si no está familiarizado con el procedimiento general de actualización de vSphere, primero debe consultar el documento *Actualización de vSphere*.

Nota Si no se respeta la secuencia de tareas para la actualización que se describe aquí, se perderán datos y se producirán errores en el clúster.

La actualización del clúster de vSAN se lleva a cabo en la siguiente secuencia de tareas.

1 Actualización de vCenter Server. Consulte la documentación sobre la *actualización de vSphere*.

2 Actualización de los hosts ESXi hosts. Consulte Actualizar los hosts ESXi. Para obtener información sobre la migración y la preparación para la actualización de los hosts ESXi, consulte el documento *Actualización de vSphere*.

3 Actualice el formato de disco de vSAN. La actualización del formato de disco es opcional, pero, para obtener los mejores resultados, actualice los objetos a la versión más reciente. El formato en disco expone el entorno al conjunto completo de características de vSAN. Consulte Actualizar el formato de disco de vSAN mediante RVC.

Lea los siguientes temas a continuación:

- Antes de actualizar vSAN
- Actualizar vCenter Server
- Actualizar los hosts ESXi
- Acerca del formato de disco de vSAN
- Acerca del formato de objetos de vSAN
- Comprobar la actualización del clúster de vSAN

- Usar las opciones del comando de actualización de RVC durante la actualización del clúster de vSAN
- Recomendaciones de compilación de vSAN para vSphere Lifecycle Manager

Antes de actualizar vSAN

Planifique y diseñe la actualización para que sea a prueba de errores.

Antes de intentar actualizar vSAN, compruebe que el entorno cumpla con los requisitos de hardware y software de vSphere.

Requisito previo de actualización

Tenga en cuenta los aspectos que pueden retrasar el proceso general de actualización. Para obtener instrucciones y prácticas recomendadas, consulte el documento *Actualización de vSphere*.

Consulte los requisitos clave antes de actualizar su clúster.

Tabla 12-1. Requisito previo de actualización

Requisitos previos de actualización	Descripción
Software, hardware, controladores, firmware y controladores de E/S de almacenamiento	Compruebe que la nueva versión de vSAN sea compatible con los componentes de software y hardware, los controladores, el firmware y los controladores de E/S de almacenamiento que planea usar. Los elementos compatibles se enumeran en el sitio web de la guía de compatibilidad de VMware en http://www.vmware.com/resources/compatibility/search.php.
Versión de vSAN	Compruebe que esté usando la versión más reciente de vSAN. No puede actualizar de una versión beta a la nueva versión de vSAN. Cuando se actualiza desde una versión beta, se debe realizar una implementación nueva de vSAN.
Espacio en disco	Compruebe que tenga espacio suficiente disponible para completar la actualización de la versión de software. La cantidad de almacenamiento en disco que se necesita para la instalación de vCenter Server depende de la configuración de vCenter Server. Para obtener instrucciones sobre el espacio en disco que se necesita para la actualización de vSphere, consulte el documento *Actualización de vSphere* .
Formato de disco de vSAN	El formato de disco de vSAN es una actualización de metadatos que no requiere evacuación ni reconstrucción de datos.

Tabla 12-1. Requisito previo de actualización (continuación)

Requisitos previos de actualización	Descripción
Hosts de vSAN	Asegúrese de haber puesto los hosts de vSAN en modo de mantenimiento y de haber seleccionado la opción **Garantizar accesibilidad a los datos** o **Evacuar todos los datos**. Puede usar vSphere Lifecycle Manager para automatizar y probar el proceso de actualización. Sin embargo, cuando se usa vSphere Lifecycle Manager para actualizar vSAN, el modo de evacuación predeterminado es **Garantizar accesibilidad a los datos**. Cuando se usa el modo **Garantizar accesibilidad a los datos**, los datos no quedan protegidos y, si ocurre un error durante la actualización de vSAN, es posible que se produzca una pérdida de datos inesperada. No obstante, el modo **Garantizar accesibilidad a los datos** es más rápido que el modo **Evacuar todos los datos**, ya que no es necesario transferir todos los datos a otro host del clúster. Para obtener información sobre diversos modos de evacuación, consulte la documentación de *Administrar VMware vSAN*.
Máquinas virtuales	Compruebe que se haya creado una copia de seguridad de las máquinas virtuales.

Recomendaciones

Tenga en cuenta las siguientes recomendaciones al implementar hosts ESXi para su uso con vSAN:

- Si los hosts de ESXi están configurados con una capacidad de memoria de 512 GB o menos, use dispositivos SATADOM, SD, USB o discos duros como medios de instalación.
- Si los hosts de ESXi están configurados con una capacidad de memoria superior a 512 GB, use un dispositivo flash o un disco magnético independiente como dispositivo de instalación. Si usa un dispositivo independiente, compruebe que vSAN no reclama el dispositivo.
- Al arrancar un host vSAN desde un dispositivo SATADOM, debe usar un dispositivo de celdas de un solo nivel (single-level cell, SLC) y el tamaño del dispositivo de arranque debe ser de 16 GB como mínimo.
- Para asegurarse de que el hardware cumpla con los requisitos de vSAN, consulte *Planificar e implementar vSAN*.

vSAN 6.5 y las versiones posteriores permiten ajustar los requisitos de tamaño de arranque para un host ESXi en un clúster de vSAN.

Actualizar el host testigo en un clúster ampliado de vSAN o de dos hosts

El host testigo de un clúster de dos hosts o un clúster ampliado de vSAN se encuentra fuera del clúster de vSAN, pero se administra con la misma instancia de vCenter Server. Es posible usar el mismo proceso para actualizar el host testigo que se usa para un host de datos de vSAN.

Actualice el host testigo antes de actualizar los hosts de datos.

El uso de vSphere Lifecycle Manager para actualizar hosts en paralelo puede provocar que el host testigo se actualice en paralelo con uno de los hosts de datos. Para evitar problemas de actualización, configure vSphere Lifecycle Manager de modo que no actualice el host testigo en paralelo con los hosts de datos.

Actualizar vCenter Server

La primera tarea que se realizará durante la actualización de vSAN es una actualización general de vSphere, que incluye la actualización de vCenter Server y los hosts ESXi.

VMware admite actualizaciones locales en sistemas de 64 bits de vCenter Server 4.x, vCenter Server 5.0.x, vCenter Server 5.1.x y vCenter Server 5.5 a vCenter Server 6.0 y posteriores. La actualización de vCenter Server incluye una actualización del esquema de la base de datos y una actualización de vCenter Server.

Los detalles y el nivel de compatibilidad para una actualización a ESXi 7.0 dependen del host que se desea actualizar y el método de actualización que utiliza. Compruebe la compatibilidad de la ruta de acceso de actualización de su versión actual de ESXi a la versión a la cual desea actualizar. Para obtener más información, consulte las Matrices de interoperabilidad de productos de VMware en http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

En lugar de realizar una actualización local a vCenter Server, se puede utilizar otro equipo para llevar a cabo la actualización. Para obtener instrucciones detalladas y varias opciones de actualización, consulte el documento *Actualizar vCenter Server*.

Actualizar los hosts ESXi

Después de actualizar vCenter Server, la siguiente tarea en la actualización del clúster de vSAN es actualizar los hosts ESXi para que usen la versión actual.

Puede actualizar los hosts ESXi en el clúster de vSAN mediante:

- vSphere Lifecycle Manager: mediante el uso de imágenes o líneas base, vSphere Lifecycle Manager permite actualizar hosts ESXi en el clúster de vSAN. El modo de evacuación predeterminado es **Garantizar accesibilidad a los datos**. Si se utiliza este modo y se produce un error durante la actualización de vSAN, es posible que no se pueda acceder a los datos hasta que uno de los hosts vuelva a estar conectado. Para obtener información sobre cómo trabajar con los modos de evacuación y mantenimiento, consulte Trabajar con miembros del clúster de vSAN en modo de mantenimiento. Para obtener más información sobre la actualización, consulte el documento *Administrar el ciclo de vida de clústeres y hosts*.
- Comando Esxcli: puede utilizar componentes, imágenes base y complementos como nuevas entregas de software para actualizar o aplicar revisiones a hosts ESXi 7.0 mediante la actualización manual.

Cuando se actualiza un clúster de vSAN con dominios de errores configurados, vSphere Lifecycle Manager actualiza un host en un solo dominio de errores y, a continuación, pasa al siguiente host. Esto garantiza que el clúster tenga las mismas versiones de vSphere que se ejecutan en todos los hosts. Cuando se actualiza un clúster ampliado de vSAN, vSphere Lifecycle Manager actualiza todos los hosts del sitio preferido y, a continuación, pasa al host en el sitio secundario. Esto garantiza que el clúster tenga las mismas versiones de vSphere que se ejecutan en todos los hosts. Para obtener más información sobre la actualización de un clúster ampliado de vSAN, consulte el documento *Administrar el ciclo de vida de clústeres y hosts*.

Antes de intentar realizar una actualización de los hosts ESXi, consulte las prácticas recomendadas que se describen en el documento *Actualización de vSphere*. VMware proporciona varias opciones de actualización de ESXi. Seleccione la opción de actualización que resulte más adecuada para el tipo de host que va a actualizar. Para obtener instrucciones detalladas y varias opciones de actualización, consulte el documento *Actualizar ESXi de VMware*.

Pasos siguientes

1 (opcional) Actualice el formato de disco de vSAN. Consulte Actualizar el formato de disco de vSAN mediante RVC.

2 Compruebe la licencia del host. En la mayoría de los casos, deberá volver a aplicar la licencia del host. Para obtener información acerca de cómo aplicar licencias de hosts, consulte el documento sobre la *administración de vCenter Server y hosts*.

3 (opcional) Actualice las máquinas virtuales en los hosts mediante vSphere Client o vSphere Lifecycle Manager.

Acerca del formato de disco de vSAN

Después de completar la actualización de ESXi, actualice el formato en disco de vSAN para acceder al conjunto completo de funciones de vSAN.

Cada versión de vSAN admite el formato en disco de las versiones anteriores. Todos los hosts del clúster deben tener la misma versión de formato en disco. Como algunas funciones están vinculadas a la versión del formato en disco, es mejor actualizar el formato en disco de vSAN a la versión más reciente compatible con la versión de ESXi. Para obtener más información, consulte https://kb.vmware.com/s/article/2148493.

La versión 3 y posteriores del formato en disco de vSAN solo requieren una actualización de metadatos que tarda unos minutos. No son necesarias la evacuación ni la reconfiguración de los discos durante la actualización del formato en disco.

Antes de actualizar el formato en disco de vSAN, ejecute la función **Comprobación previa de actualización** para garantizar que la actualización se realice sin problemas. La comprobación previa permite identificar posibles problemas que podrían impedir que la actualización se realice correctamente, como discos con errores u objetos en mal estado.

Nota Una vez que actualice el formato en disco, no podrá revertir el software en los hosts o agregar determinados hosts más antiguos al clúster.

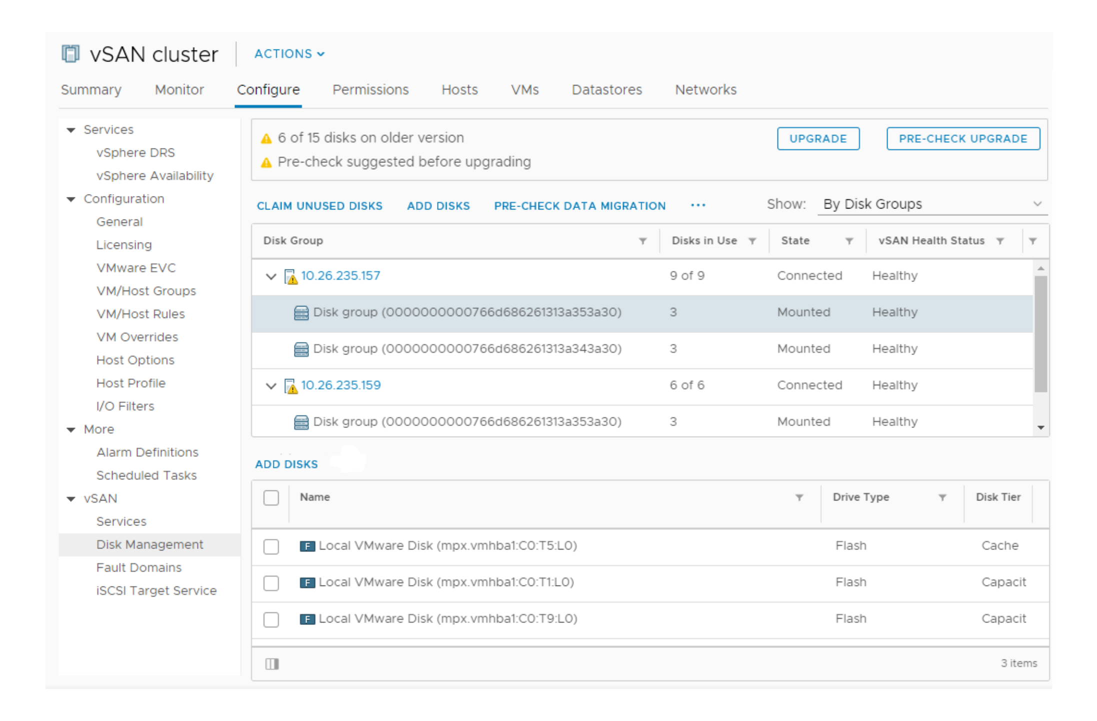
Actualizar el formato de disco de vSAN mediante vSphere Client

Una vez que haya terminado de actualizar los hosts de vSAN, puede realizar la actualización del formato de disco.

Nota Si habilita el cifrado o la desduplicación y la compresión en un clúster de vSAN existente, el formato en disco se actualiza automáticamente a la versión más reciente. Este procedimiento no es obligatorio. Consulte Editar la configuración de vSAN.

Requisitos previos

- Compruebe que esté usando la versión actualizada de vCenter Server.
- Compruebe que esté usando la versión más reciente de los hosts ESXi.
- Compruebe que los discos se encuentren en buen estado. Desplácese hasta la página Administración de discos para comprobar el estado del objeto.
- Compruebe que los componentes de hardware y software que planea usar estén certificados y aparezcan en el sitio web de la guía de compatibilidad de VMware, a la cual puede acceder mediante la siguiente URL: http://www.vmware.com/resources/compatibility/search.php.
- Compruebe que tenga espacio suficiente para ejecutar la actualización del formato de disco. Ejecute el comando de RVC, `vsan.whatif_host_failures`, para determinar si dispone de capacidad suficiente para completar correctamente la actualización o recompilar los componentes en caso de que haya errores durante la actualización.
- Compruebe que los hosts no estén en modo de mantenimiento. Al actualizar el formato de disco, no coloque los hosts en el modo de mantenimiento. Cuando un host miembro de un clúster de vSAN entra en modo de mantenimiento, el host miembro deja de aportar capacidad al clúster. Se reduce la capacidad del clúster y se puede producir un error en la actualización del clúster.
- Compruebe que no haya tareas de recompilación de componentes en curso en el clúster de vSAN. Para obtener información acerca de la resincronización de vSAN, consulte *Supervisión y rendimiento de vSphere*.



Procedimiento

1. Desplácese hasta el clúster de vSAN.
2. Haga clic en la pestaña **Configurar**.
3. En vSAN, seleccione **Administración de discos**.
4. (Opcional) Haga clic en **Comprobación previa de actualización**.

   La comprobación previa de actualización analizará el clúster para detectar problemas que puedan evitar que la actualización se realice correctamente. Algunos de los elementos que se comprueban son el estado del host, el estado del disco, el estado de la red y el estado de los objetos. Los problemas de actualización se muestran en el cuadro de texto **Estado de comprobación previa de disco**.
5. Haga clic en **Actualizar**.
6. Haga clic en **Sí** en el cuadro de diálogo Actualizar para realizar la actualización del formato en disco.

Resultados

vSAN actualiza correctamente el formato en disco. La columna On-disk Format Version (Versión de formato en disco) muestra la versión del formato de disco de los dispositivos de almacenamiento del clúster.

Si ocurre un error durante la actualización, puede comprobar la página Resincronización de componentes. Espere a que se complete la resincronización y vuelva a ejecutar la actualización. También puede comprobar el estado del clúster mediante el servicio de estado. Después de resolver cualquier problema que haya surgido a partir de las comprobaciones de estado, puede volver a ejecutar la actualización.

Actualizar el formato de disco de vSAN mediante RVC

Una vez que haya terminado de actualizar los hosts de vSAN, puede usar la herramienta Ruby vSphere Console (RVC) para continuar con la actualización del formato de disco.

Requisitos previos

- Compruebe que esté usando la versión actualizada de vCenter Server.
- Compruebe que la versión de los hosts ESXi que se ejecutan en el clúster de vSAN sea la versión 6.5 o una versión posterior.
- Compruebe que los discos estén en buen estado desde la página Administración de discos. También puede ejecutar el comando de RVC `vsan.disks_stats` para comprobar el estado del disco.
- Compruebe que los componentes de hardware y software que planea usar estén certificados y aparezcan en el sitio web de la guía de compatibilidad de VMware, a la cual puede acceder mediante la siguiente URL: http://www.vmware.com/resources/compatibility/search.php.
- Compruebe que tenga espacio suficiente para ejecutar la actualización del formato de disco. Ejecute el comando `vsan.whatif_host_failures` de RVC para determinar si dispone de capacidad suficiente para completar la actualización o realizar una recompilación de componentes en caso de que se produzcan errores durante la actualización.
- Compruebe que PuTTY o un cliente SSH similar estén instalados para acceder a la herramienta RVC.

  Para obtener información detallada sobre la descarga de la herramienta RVC y sobre el uso de comandos de RVC, consulte la *Guía de referencia de los comandos de RVC*.
- Compruebe que los hosts no estén en modo de mantenimiento. Al actualizar el formato en disco, no coloque los hosts en el modo de mantenimiento. Cuando cualquier host miembro de un clúster de vSAN entra en modo de mantenimiento, la capacidad de recursos disponible se reduce porque el host miembro deja de aportar capacidad al clúster. Es posible que se produzca un error en la actualización del clúster.
- Compruebe que no haya tareas de recompilación de componentes en curso en el clúster de vSAN mediante la ejecución del comando de RVC `vsan.resync_dashboard`.

Procedimiento

1. Inicie sesión en vCenter Server con la herramienta RVC.
2. Ejecute el siguiente comando de RVC para ver el estado del disco: `vsan.disks_stats /<vCenter IP address or hostname>/<data center name>/computers/<cluster name>`

   Por ejemplo: `vsan.disks_stats /192.168.0.1/BetaDC/computers/VSANCluster`

   El comando enumera los nombres de todos los dispositivos y los hosts del clúster de vSAN. El comando también muestra el formato de disco actual y su estado de mantenimiento. También puede comprobar el estado actual de los dispositivos de la columna **Health Status**

(Estado de mantenimiento) de la página **Disk Management** (Administración de discos). Por ejemplo, el estado del dispositivo que se muestra es Unhealthy (Estado incorrecto) en la columna **Health Status** (Estado de mantenimiento) para los hosts o los grupos de discos que tienen dispositivos que presentan errores.

3 Ejecute el siguiente comando de RVC: `vsan.ondisk_upgrade <path to vsan cluster>`

   Por ejemplo: `vsan.ondisk_upgrade /192.168.0.1/BetaDC/computers/VSANCluster`

4 Supervise el progreso en RVC.

   RVC actualiza un grupo de discos a la vez.

   Una vez que la actualización del formato de disco finalice correctamente, aparecerá el siguiente mensaje:

```
Done with disk format upgrade phase (Finalizó la fase de actualización del formato de
disco)
```

```
There are n v1 objects that require upgrade Object upgrade progress: n upgraded, 0
left (Hay n objetos de v1 que requieren una actualización. Progreso de actualización de
objetos: n actualizados, 0 restantes)
```

```
n upgraded (Finalizó la actualización de objetos: n actualizados)
```

```
Done VSAN upgrade (Finalizó la actualización de VSAN)
```

5 Ejecute el siguiente comando de RVC para verificar que las versiones de los objetos se actualizaron al nuevo formato en disco: `vsan.obj_status_report`

Comprobar la actualización del formato de disco de vSAN

Una vez finalizada la actualización del formato de disco, debe comprobar si el clúster de vSAN está usando el nuevo formato en disco.

Procedimiento

1 Desplácese hasta el clúster de vSAN.

2 Haga clic en la pestaña **Configurar**.

3 En vSAN, haga clic en **Administración de discos**.

   La versión actual del formato de disco aparece en la columna Disk Format Version (Versión de formato de disco).

Acerca del formato de objetos de vSAN

El espacio de operaciones que necesita vSAN para realizar un cambio de directiva u otras operaciones de este tipo en un objeto creado por vSAN 7.0 o una versión anterior es el espacio utilizado por un objeto más grande en el clúster.

Por lo general, esto resulta difícil de planificar y, por lo tanto, la norma era mantener un 30 % de espacio libre en el clúster, asumiendo que es improbable que el objeto más grande del clúster consume más del 25 % del espacio y que el 5 % del espacio está reservado para asegurarse de que el clúster no se llene debido a cambios en la directiva. En vSAN 7.0 U1 y versiones posteriores, todos los objetos se crean en un formato nuevo que permite que el espacio de operaciones que necesita vSAN realice cambios de directiva en un objeto si hay 255 GB por host para objetos inferiores a 8 TB y 765 GB por host para objetos de 8 TB o más.

Después de actualizar un clúster a vSAN 7.0 U1 o versiones posteriores desde vSAN 7.0 o una versión anterior, los objetos de más de 255 GB creados con la versión anterior se deben volver a escribir en el nuevo formato antes de que vSAN permita realizar operaciones en un objeto con los nuevos requisitos de espacio libre. Después de una actualización, se muestra una alerta de estado de nuevo formato de objeto después de una actualización, si hay objetos que deben cambiar al nuevo formato de objeto, y permite que el estado de mantenimiento se corrija iniciando una tarea de rediseño para arreglar estos objetos. La alerta de mantenimiento proporciona información sobre el número de objetos que se deben fijar y la cantidad de datos que se reescribirán. Es posible que el clúster experimente un descenso del 20 % del rendimiento mientras la tarea de rediseño está en curso. El panel de resincronización proporciona información más precisa sobre el tiempo que tardará esta operación en completarse.

Comprobar la actualización del clúster de vSAN

La actualización del clúster de vSAN no finalizará hasta que compruebe que está usando la versión más reciente de vSphere y que vSAN está disponible para su uso.

Procedimiento

1 Desplácese hasta el clúster de vSAN.

2 Haga clic en la pestaña **Configure** (Configurar) y compruebe que aparezca vSAN.

  - También puede desplazarse hasta el host ESXi y seleccionar **Summary** (Resumen) > **Configuration** (Configuración) y comprobar que utiliza la versión más reciente del host ESXi.

Usar las opciones del comando de actualización de RVC durante la actualización del clúster de vSAN

El comando `vsan.ondisk_upgrade` proporciona diversas opciones de comando que pueden utilizarse para controlar y administrar la actualización del clúster de vSAN.

Por ejemplo, puede permitir una redundancia reducida para realizar la actualización cuando tenga un poco de espacio libre disponible. Ejecute el comando `vsan.ondisk_upgrade --help` para visualizar la lista de las opciones de comandos de RVC.

Use estas opciones de comandos con el comando `vsan.ondisk_upgrade`.

Tabla 12-2. Opciones de comandos de actualización

Opciones	Descripción
`--hosts_and_clusters`	Use esta opción para especificar rutas de acceso a todos los sistemas host del clúster o los recursos informáticos del clúster.
`--ignore-objects, -i`	Use esta opción para omitir la actualización de un objeto de vSAN. También puede usar esta opción de comando para eliminar la actualización de la versión de un objeto. Cuando use esta opción de comando, los objetos continuarán utilizando la versión de formato en disco actual.
`--allow-reduced-redundancy, -a`	Use esta opción para eliminar la necesidad de contar con espacio libre equivalente a un grupo de discos durante la actualización de discos. Con esta opción, las máquinas virtuales funcionan en modo de redundancia reducida durante la actualización, lo que significa que es posible que ciertas máquinas virtuales no toleren errores temporalmente, y esta incapacidad puede producir pérdida de datos. vSAN restaura la redundancia y el cumplimiento completos una vez finalizada la actualización.
`--force, -f`	Use esta opción para permitir forzar el procedimiento y responder automáticamente todas las preguntas de confirmación.
`--help, -h`	Use esta opción para mostrar las opciones de ayuda.

Para obtener información sobre el uso de los comandos de RVC, consulte la *Guía de referencia de los comandos de RVC*.

Recomendaciones de compilación de vSAN para vSphere Lifecycle Manager

vSAN genera líneas base del sistema y grupos de líneas base que puede usar con vSphere Lifecycle Manager.

vSphere Lifecycle Manager en vSphere 7.0 incluye las líneas base del sistema que proporcionaba Update Manager en versiones de vSphere anteriores. También incluye una nueva función de administración de imágenes para los hosts que ejecutan ESXi 7.0 y versiones posteriores.

vSAN 6.6.1 y las versiones posteriores generan recomendaciones de compilación automatizadas para los clústeres de vSAN. vSAN combina información de la guía de compatibilidad de VMware y del catálogo de versiones de vSAN con información sobre las versiones de ESXi instaladas. Estas actualizaciones recomendadas proporcionan la mejor versión disponible para asegurarse de que el hardware se mantenga en un estado admitido.

Las líneas base del sistema desde vSAN 6.7.1 hasta vSAN 7.0 también pueden incluir actualizaciones de firmware y de controladores de dispositivos. Estas actualizaciones admiten el software de ESXi recomendado para el clúster.

En vSAN 6.7.3 y versiones posteriores, puede elegir que se proporcionen recomendaciones de compilación solo para la versión actual de ESXi o para la versión más reciente de ESXi admitida. Una recomendación de compilación para la versión actual incluye todas las revisiones y las actualizaciones de los controladores correspondientes a la versión.

En vSAN 7.0 y versiones posteriores, las recomendaciones de compilación de vSAN incluyen actualizaciones de revisiones y actualizaciones de controladores aplicables. Para actualizar el firmware en clústeres de vSAN 7.0, debe utilizar una imagen a través de vSphere Lifecycle Manager.

Líneas base del sistema de vSAN

Las recomendaciones de compilación de vSAN se proporcionan a través de las líneas base del sistema de vSAN para vSphere Lifecycle Manager. vSAN administra estas líneas base del sistema. Son de solo lectura y no se pueden personalizar.

vSAN genera un grupo de líneas base para cada clúster de vSAN. Las líneas base del sistema de vSAN se enumeran en el panel **Líneas base** de la pestaña Líneas base y grupos. Puede seguir creando y corrigiendo sus propias líneas base.

Las líneas base del sistema de vSAN pueden incluir imágenes ISO personalizadas proporcionadas por proveedores certificados. Si los hosts del clúster de vSAN tienen imágenes ISO personalizadas que son específicas de OEM, las líneas base del sistema recomendadas por vSAN pueden incluir imágenes ISO personalizadas del mismo proveedor. vSphere Lifecycle Manager no puede generar una recomendación para imágenes ISO personalizadas no admitidas por vSAN. Si ejecuta una imagen de software personalizado que reemplaza el nombre del proveedor en el perfil de imagen del host, vSphere Lifecycle Manager no puede recomendar una línea base del sistema.

vSphere Lifecycle Manager examina cada clúster de vSAN de forma automática para comparar el cumplimiento con el grupo de líneas base. Para actualizar el clúster, debe corregir de forma manual la línea base del sistema mediante vSphere Lifecycle Manager. Es posible corregir la línea base del sistema de vSAN en un único host o en todo el clúster.

Catálogo de versiones de vSAN

El catálogo de versiones de vSAN contiene información sobre las versiones disponibles, el orden de preferencia de las versiones y las revisiones esenciales necesarias para cada versión. El catálogo de versiones de vSAN se hospeda en VMware Cloud.

vSAN requiere conectividad a Internet para acceder al catálogo de versiones. No es necesario que esté inscrito en el Programa de mejora de la experiencia de cliente (Customer Experience Improvement Program, CEIP) para que vSAN pueda acceder al catálogo de versiones.

Si no tiene una conexión a Internet, puede cargar el catálogo de versiones de vSAN directamente en vCenter Server. En vSphere Client, haga clic en **Configurar > vSAN > Actualizar** y en **Cargar desde archivo** en la sección Catálogo de versiones. Puede descargar el catálogo de versiones de vSAN más reciente.

vSphere Lifecycle Manager le permite importar controladores de los controladores de almacenamiento recomendados para el clúster de vSAN. Algunos proveedores de controladores de almacenamiento ofrecen una herramienta de administración de software que vSAN puede usar para actualizar los controladores de los controladores de almacenamiento. Si los hosts ESXi no incluyen la herramienta de administración, es posible descargarla.

Trabajar con las recomendaciones de compilación de vSAN

vSphere Lifecycle Manager compara las versiones de ESXi instaladas con la información de la lista de compatibilidad de hardware (Hardware Compatibility List, HCL) en la guía de compatibilidad de VMware. Determina la ruta de acceso de actualización correcta para cada clúster de vSAN con base en el catálogo de versiones de vSAN actual. vSAN también incluye las actualizaciones de revisión y los controladores necesarios para la versión recomendada en su línea base del sistema.

Las recomendaciones de compilación de vSAN garantizan que cada clúster de vSAN permanezca en el estado de compatibilidad de hardware actual o superior. Si el hardware en el clúster de vSAN no está incluido en la HCL, vSAN puede recomendar una actualización a la versión más reciente, ya que no es peor que el estado actual.

Nota vSphere Lifecycle Manager utiliza el servicio de estado de vSAN cuando realiza la comprobación previa de corrección de hosts en un clúster de vSAN. El servicio de estado de vSAN no está disponible en los hosts que ejecutan ESXi 6. 0 Update 1 o una versión anterior. Cuando vSphere Lifecycle Manager actualiza los hosts que ejecutan ESXi 6.0 Update 1 o una versión anterior, la actualización del último host del clúster de vSAN puede fallar. Si la corrección no se realizó correctamente debido a problemas de estado de vSAN, aún es posible completar la actualización. Utilice el servicio de estado de vSAN para solucionar los problemas de estado en el host y, a continuación, saque al host del modo de mantenimiento para completar el flujo de trabajo de actualización.

Los siguientes ejemplos describen la lógica utilizada por las recomendaciones de compilación de vSAN.

Ejemplo 1

Un clúster de vSAN ejecuta la versión 6.0 Update 2 y su hardware se encuentra en la HCL de la versión 6.0 Update 2. La HCL muestra que el hardware es compatible hasta la versión 6.0 Update 3, pero no para las versiones 6.5 y posteriores. vSAN recomienda una actualización a la versión 6.0 Update 3, incluidas las revisiones esenciales que necesita la versión.

Ejemplo 2

Un clúster de vSAN ejecuta la versión 6.7 Update 2 y su hardware se encuentra en la HCL de la versión 6.7 Update 2. El hardware también se admite en la HCL de la versión 7.0 Update 3. vSAN recomienda una actualización a la versión 7.0 Update 3.

Ejemplo 3

Un clúster de vSAN ejecuta la versión 6.7 Update 2 y su hardware no se encuentra en la HCL de dicha versión. vSAN recomienda una actualización a la versión 7.0 Update 3, a pesar de que el hardware no aparece en la HCL de la versión 7.0 Update 3. vSAN recomienda la actualización porque el nuevo estado no es peor que el estado actual.

Ejemplo 4

Un clúster de vSAN ejecuta la versión 6.7 Update 2 y su hardware se encuentra en la HCL de la versión 6.7 Update 2. El hardware también es compatible con la HCL para la versión 7.0 Update 3; la preferencia de línea base seleccionada es solo de revisión. vSAN recomienda una actualización a la versión 7.0 Update 3, incluidas las revisiones esenciales que necesita la versión.

El motor de recomendaciones se ejecuta periódicamente (una vez al día) o cuando ocurren los siguientes eventos.

- La pertenencia al clúster cambia. Por ejemplo, cuando se agrega o se quita un host.
- El servicio de administración de vSAN se reinicia.
- Un usuario inicia sesión en VMware Customer Connect con un navegador web o con RVC.
- Se realiza una actualización en la guía de compatibilidad de VMware o en el catálogo de versiones de vSAN.

La comprobación de estado de la recomendación de compilación de vSAN muestra la compilación actual que se recomienda para el clúster de vSAN. También puede avisarle de cualquier problema existente en la función.

Requisitos del sistema

vSphere Lifecycle Manager es un servicio de extensión en vCenter Server 7.0 y versiones posteriores.

vSAN requiere acceso a Internet para actualizar los metadatos de la versión, para comprobar la guía de compatibilidad de VMware y para descargar las imágenes ISO desde VMware Customer Connect.

vSAN requiere credenciales válidas para descargar imágenes ISO correspondientes a las actualizaciones desde VMware Customer Connect. En los hosts que ejecutan la versión 6.0 Update 1 o una anterior, debe usar RVC para introducir las credenciales de **VMware Customer Connect**. En los hosts que ejecutan software de una versión posterior, puede iniciar sesión desde la comprobación de estado de la recomendación de compilación de ESX.

Para introducir las credenciales de **VMware Customer Connect** desde RVC, ejecute el siguiente comando: **`vsan.login_iso_depot -u`** *<nombre de usuario>* **`-p`** *<contraseña>*